Comprobaciones de compatibilidad con Nessus

Auditorías de contenido y configuraciones de sistemas

14 de enero de 2014

(Revisión 74)

Índice

Introducción

Este documento describe la forma en que Nessus 5.x se puede usar para auditar la configuración de sistemas Unix, Windows, de bases de datos, SCADA, IBM iSeries y Cisco respecto de una directiva de compatibilidad, así como examinar distintos sistemas en busca de contenido confidencial.

En el presente documento, las frases “Compatibilidad con directivas” y “Comprobaciones de compatibilidad” se usan indistintamente.

Las auditorías de sistemas SCADA son posibles en Nessus. No obstante, esta función se encuentra fuera del alcance de lo cubierto en el presente documento. Consulte la página de información Tenable SCADA aquí para obtener más información.

Llevar a cabo una auditoría de compatibilidad no es lo mismo que realizar un análisis de vulnerabilidades, a pesar de que puede producirse cierta superposición. Una auditoría de compatibilidad determina si un sistema se configuró de acuerdo con una directiva establecida. Un análisis de vulnerabilidades determina si el sistema es propenso a vulnerabilidades conocidas. Los lectores conocerán los tipos de parámetros de configuración y datos confidenciales que se pueden auditar, y aprenderán a configurar Nessus para realizar estas auditorías y la forma en que el SecurityCenter de Tenable se puede usar para administrar y automatizar este proceso.

Requisitos previos

Este documento supone cierto nivel de conocimiento sobre el analizador de vulnerabilidades Nessus. Para obtener más información sobre cómo Nessus puede configurarse para realizar auditorías de revisiones locales para Unix y Windows, consulte el documento “Nessus Credentials Checks for Unix and Windows” (“Comprobaciones con credenciales de Nessus para Unix y Windows”), que puede encontrar en http://www.tenable.com/products/nessus/documentation.

Clientes de Nessus and SecurityCenter

Los usuarios deben estar inscritos en Nessus comercial o usar SecurityCenter para realizar las comprobaciones de compatibilidad que se describen en este documento. Ambos se encuentran disponibles en Tenable Network Security (http://www.tenable.com/). En los próximos capítulos se abordará una lista más detallada de los requisitos técnicos necesarios para llevar a cabo las comprobaciones de auditoría.

Estándares y convenciones

En toda la documentación, los nombres de archivo, demonios y archivos ejecutables se indican con fuente **`courier negrita`**.

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.

Estándares de compatibilidad

Existen muchos tipos diversos de requisitos de compatibilidad gubernamentales y financieros. Resulta importante comprender que estos requisitos de compatibilidad constituyen bases mínimas, que se pueden interpretar de forma diferente de acuerdo con las metas empresariales de la organización. Los requisitos de compatibilidad deben asociarse con las metas empresariales para garantizar que los riesgos se identifiquen y mitiguen correctamente. Para obtener más información sobre cómo desarrollar este proceso, consulte el documento de Tenable "Maximizing ROI on Vulnerability Management" (Cómo maximizar el retorno de la inversión en la administración de vulnerabilidades), que se puede encontrar en http://www.tenable.com/whitepapers.

Por ejemplo, en una empresa puede haber una directiva que exija que todos los servidores que contengan "Personally identifiable information, PII" (Información de identificación personal) de clientes tengan registro habilitado y contraseñas con longitudes de 10 caracteres como mínimo. Esta directiva puede ser de ayuda para los esfuerzos de una organización tendientes a mantener la compatibilidad con una serie de reglamentaciones diferentes.

Algunas de las reglamentaciones y guías de compatibilidad comunes son:

- BASEL II
- Center for Internet Security Benchmarks (CIS) (Criterios de referencia del Center for Internet Security [CIS])
- Control Objectives for Information and related Technology (COBIT) (Objetivos de control para la tecnología de la información y otras tecnologías relacionadas [COBIT])
- Defense Information Systems Agency (DISA) STIGs (Guías de implementación técnica de seguridad [STIG] de la Agencia de Sistemas de Información de Defensa [DISA])
- Federal Information Security Management Act (FISMA) (Ley de Administración de Seguridad de la Información Federal [FISMA])
- Federal Desktop Core Configuration (FDCC) (Configuración Federal Central de los equipos de escritorio [FDCC])
- Gramm-Leach-Bliley Act (GLBA) (Ley Gramm-Leach-Bliley [GLBA])
- Health Insurance Portability and Accountability Act (HIPAA) (Ley de Responsabilidad y Transferibilidad de los Seguros Médicos [HIPAA])
- Normas de seguridad ISO 27002/17799
- Information Technology Information Library (ITIL) (Biblioteca de Infraestructura de Tecnologías de la Información [ITIL])
- National Institute of Standards (NIST) configuration guidelines (Pautas de configuración del Instituto Nacional de Estándares y Tecnología [NIST])
- National Security Agency (NSA) configuration guidelines (Pautas de configuración de la Agencia Nacional de Seguridad [NSA])
- Payment Card Industry Data Security Standards (PCI DSS) (Estándares de seguridad de datos de la industria de tarjetas de pago [PCI DSS])
- Sarbanes-Oxley (SOX)
- Site Data Protection (SDP) (Protección de datos de sitios web [SDP])
- United States Government Configuration Baseline (USGCB) (Configuración básica del gobierno de los Estados Unidos [USGCB])

- Distintas leyes estatales, por ejemplo, la California's Security Breach Notification Act, SB 1386 (Ley de Notificación de incumplimiento de la seguridad de California, SB 1386)

Estas comprobaciones de compatibilidad también abordan la supervisión en tiempo real, como la realización de actividades para la detección de intrusos y el control de acceso. Para interiorizarse sobre la forma en que las soluciones de auditorías de configuración, administración de vulnerabilidades, filtración de datos, análisis de registros y supervisión de redes de Tenable pueden ayudar con las reglamentaciones de compatibilidad mencionadas, envíe un mensaje de correo electrónico a sales@tenable.com para solicitar un ejemplar del documento "Real-Time Compliance Monitoring" ("Supervisión de compatibilidad en tiempo real").

Auditorías de configuración, filtración de datos y compatibilidad

¿Qué es una auditoría?

Nessus se puede usar para iniciar sesión en servidores Unix y Windows, dispositivos Cisco, sistemas SCADA, servidores IBM iSeries y bases de datos para determinar si se configuraron de acuerdo con la directiva local de seguridad de sitios. Nessus también puede realizar una búsqueda en toda la unidad de disco duro de sistemas Windows y Unix para detectar contenido no autorizado.

Es importante que las organizaciones establezcan una directiva de seguridad de sitios antes de realizar una auditoría, para garantizar que los recursos se encuentren protegidos de forma adecuada. Una evaluación de vulnerabilidades determinará si los sistemas están expuestos a vulnerabilidades de seguridad conocidas, pero no determinará, por ejemplo, si los registros del personal se almacenan en un servidor público.

No hay una norma absoluta de seguridad, ya que la cuestión consiste en la administración de riesgos y esto varía de una organización a otra.

Por ejemplo, tenga en cuenta los requisitos de contraseñas, tales como vigencias mínimas o máximas de contraseña y directivas de bloqueo de cuentas. Pueden existir razones de mucho peso para cambiar contraseñas con mucha o poca frecuencia. También puede haber muy buenas razones para bloquear una cuenta si se produjeron más de cinco errores al iniciar sesión, pero si se trata de un sistema esencial, establecer un valor algo más alto o incluso deshabilitar todos los bloqueos podría ser más prudente.

Estos parámetros de configuración se relacionan en gran medida con la administración del sistema y la política de seguridad, pero no específicamente con vulnerabilidades del sistema ni revisiones faltantes. Nessus puede realizar comprobaciones de compatibilidad en servidores de Unix y Windows. Las directivas pueden ser muy simples o muy complejas, de acuerdo con los requisitos de cada análisis de compatibilidad individual.

Comparación entre auditorías y análisis de vulnerabilidades

Nessus puede realizar análisis de vulnerabilidades de servicios de red, así como también iniciar sesión en servidores para descubrir revisiones faltantes. Sin embargo, la falta de vulnerabilidades no supone que los servidores estén configurados correctamente o sean "compatibles" con una norma en particular.

La ventaja de usar Nessus para realizar análisis de vulnerabilidades y auditorías de compatibilidad consiste en que todos estos datos se pueden obtener a la vez. Conocer cómo está configurado un servidor, las revisiones con las que cuenta y qué vulnerabilidades están presentes puede ayudar a determinar las medidas para mitigar riesgos.

En un nivel superior, si se suma esta información para toda una red o una clase de activo (al igual que con SecurityCenter de Tenable), la seguridad y el riesgo se pueden analizar de manera global. Esto permite a los auditores y a los administradores de redes detectar tendencias en sistemas no compatibles y ajustar controles para resolverlas a una mayor escala.

Ejemplo de elementos de auditoría

Las secciones siguientes abordan las auditorías de configuración en sistemas Windows, Unix, Cisco, IBM iSeries y de bases de datos.

El motor regex de Nessus 5 tiene como base el dialecto Perl y se considera "POSIX extendido", dadas su flexibilidad y velocidad.

Todos los archivos de la auditoría deben estar codificados en formato ANSI. Los archivos codificados en Unicode, Unicode big endian y UTF-8 no funcionarán.

Windows
Nessus puede probar cualquier opción que se pueda configurar como “policy” (directiva) en el framework de Microsoft Windows. Existen centenares de opciones de registro que se pueden auditar, y también se pueden analizar los permisos de archivos, directorios y objetos. Una lista parcial de ejemplos de auditorías incluye la prueba de opciones de lo siguiente:

- Duración de bloqueo de cuenta
- Conservación de registro de seguridad
- Habilitación de inicio de sesión local
- Aplicación del historial de contraseñas

A continuación se presenta un ejemplo de elemento de “audit” (auditoría) para servidores de Windows:

```
<item>
 name: "Minimum password length"
 value: 7
</item>
```

Esta auditoría en particular busca la opción “Minimum password length” (Longitud de contraseña mínima) en un servidor de Windows, y genera una alerta si el valor es inferior a siete caracteres.

Nessus también puede buscar datos confidenciales en equipos Windows. A continuación se presenta un ejemplo que busca números de tarjeta de crédito Visa en una variedad de formatos de archivo:

```
<item>
 type: FILE_CONTENT_CHECK
 description: "Determine if a file contains a valid VISA Credit Card Number"
 file_extension: "xls" | "pdf" | "txt"
 regex: "([^0-9-]|^)(4[0-9]{3}( |-|)([0-9]{4})( |-|)([0-9]{4})( |-|)([0-9]{4}))([^0-9-
       ]|$)"
 expect: "VISA" | "credit" | "Visa" | "CCN"
 max_size: "50K"
 only_show: "4"
</item>
```

Esta comprobación analiza archivos Excel, Adobe y de texto para detectar patrones que indiquen la presencia de uno o más números de tarjeta de crédito Visa válidos.

Unix
Nessus se puede usar de manera general para probar los permisos de los archivos, el contenido de un archivo, los procesos en ejecución y el control de acceso de usuario en una variedad de sistemas basados en Unix. Actualmente se encuentran disponibles las comprobaciones para auditar Solaris, Red Hat, AIX, HP-UX, SuSE, Gentoo y FreeBSD, derivados de Unix.

```
<item>
 name: "min_password_length"
 description: "Minimum password length"
```

```
 value: "14..MAX"
</item>
```

Esta auditoría comprueba si la longitud de contraseña mínima en un sistema Unix tiene 14 caracteres.

Cisco
Nessus puede probar la configuración en ejecución de sistemas que emplean el sistema operativo Cisco IOS, y confirmar que sea compatible con los estándares de directivas de seguridad. Las comprobaciones se pueden llevar a cabo mediante un inicio de sesión sin privilegios o uno que utilice la contraseña privilegiada “enable” (habilitar).

```
<item>
 type: CONFIG_CHECK
 description: "Require AAA service"
 info: "Verify centralized authentication, authorization and accounting"
 info: "(AAA)service (new-model) is enabled."
 item: "aaa new-model"
</item>
```

Firewall de Palo Alto
Nessus utiliza XSL Transforms (XSLT) y una API nativa para solicitar información a dispositivos Palo Alto con PAN-OS. Las solicitudes se hacen a través de la interfaz HTTP o HTTPS del firewall, y requieren credenciales de administrador `Superuser (Superusuario)` o `Superuser (readonly) (Superusuario [solo lectura])` para PAN-OS >= 4.1.0 o credenciales de administrador de `Superuser (Superusuario)` para PAN-OS < 4.1.0. Esto le permite hacer auditorías a una `operational config` (configuración operativa) en el dispositivo.

```
<custom_item>
 type: AUDIT_XML
 description: "Palo Alto Security Settings - 'fips-mode = on'"
 info: "Fips-mode should be enabled."
 api_request_type: "op"
 request: "<show><fips-mode></fips-mode></show>"
 xsl_stmt: "<xsl:template match=\"/\">"
 xsl_stmt: "  <xsl:apply-templates select=\"//result\"/>"
 xsl_stmt: "</xsl:template>"
 xsl_stmt: "<xsl:template match=\"//result\">"
 xsl_stmt: "fips-mode: <xsl:value-of select=\"text()\"/>"
 regex: "fips-mode:[\\s\\t]+"
 expect: "fips-mode:[\\s\\t]+on"
</custom_item>
```

IBM iSeries
Con las credenciales suministradas, Nessus puede probar la configuración de sistemas con IBM iSeries y confirmar que cumplan con los estándares de las directivas de seguridad.

```
<custom_item>
 type: AUDIT_SYSTEMVAL
 systemvalue: "QALWUSRDMN"
 description: "Allow User Domain Objects (QALWUSRDMN) - '*all'"
 value_type: POLICY_TEXT
 value_data: "*all"
 info: "\nref :
       http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415302.pdf
       pg. 21"
```

```
</custom_item>
```

NetApp Data ONTAP
Con las credenciales suministradas, Nessus puede probar la configuración de sistemas con NetApp Data ONTAP y confirmar que cumplan con los estándares de las directivas de seguridad.

```
<custom_item>
 type: CONFIG_CHECK
 description: "1.2 Secure Storage Design, Enable Kerberos with NFS –
       'nfs.kerberos.enable = on'"
 info: "NetApp recommends the use of security features in IP storage protocols to
       secure client access"
 solution: "Enable Kerberos with NFS"
 reference: "PCI|2.2.3"
 see_also: "http://media.netapp.com/documents/tr-3649.pdf"
 regex: "nfs.kerberos.enable[\\s\\t]+"
 expect: "nfs.kerberos.enable[\\s\\t]+on"
</custom_item>
```

Bases de datos
Nessus se puede configurar para iniciar sesión y determinar la compatibilidad con las directivas de seguridad locales en los siguientes tipos de bases de datos:

- SQL Server
- Oracle
- MySQL
- PostgreSQL
- DB2
- Informix/DRDA

En general, Tenable recomienda ejecutar un análisis de compatibilidad de base de datos con un usuario con privilegios SYSDBA para Oracle, "**sa**" o una cuenta con la función de servidor sysadmin para MS-SQL y una cuenta de usuario de instancia de DB2 para DB2 para garantizar la totalidad del informe, ya que algunos parámetros y tablas de sistema u ocultas solo pueden accederse por medio de una cuenta con dichos privilegios. Tenga en cuenta que para Oracle, en la mayoría de los casos, un usuario que tiene asignada la función DBA hará la mayoría de las comprobaciones en las auditorías de Tenable, pero algunas comprobaciones informarán errores debido a la falta de privilegios de acceso. El mismo argumento es aplicable a otras bases de datos; una cuenta con menos privilegios podría utilizarse para la auditoría de la base de datos, pero la desventaja es que no se puede garantizar un informe completo.

Las auditorías de bases de datos constan normalmente de instrucciones específicas que recuperan de su base de datos detalles relacionados con la seguridad, como la existencia o el estado de procedimientos almacenados de forma insegura. A continuación se incluye un ejemplo que determina si el procedimiento almacenado "**xp_cmdshell**", posiblemente peligroso, se encuentra habilitado:

```
<custom_item>
 type: SQL_POLICY
 description: "xp_cmdshell option"
 info: "The xp_cmdshell extended stored procedures allows execution of host
       executables outside the controls of database access permissions and may be
       exploited by malicious users."
 info: "Checking that the xp_cmdshell stored procedure is set to '0'"
 sql_request: "select value_in_use from sys.configurations where name = 'xp_cmdshell'"
 sql_types: POLICY_INTEGER
```

```
  sql_expect: "0"
</custom_item>
```

La capacidad de escribir archivos de auditoría para cada organización y buscar datos confidenciales resulta muy útil. Este documento describe la forma de crear directivas personalizadas para buscar distintos tipos de datos.

Informes de auditoría

Cuando se lleva a cabo una auditoría, Nessus intenta determinar si el host es compatible, no compatible, o si los resultados no son concluyentes.

Los resultados de compatibilidad se registran en Nessus como “Pass” (Aprobado), “Fail” (Desaprobado) y “Warning” (Advertencia). La interfaz del usuario de Nessus y SecurityCenter de Tenable registran los resultados como “Info” en el caso de que se hayan aprobado, “High” (Alta) si desaprobaron y “Medium” (Media) para resultados no concluyentes (por ejemplo, una comprobación de permisos de un archivo que no se encontró en el sistema).

A diferencia de la comprobación de vulnerabilidades, que solo informa si la vulnerabilidad se encuentra efectivamente presente, una comprobación de compatibilidad siempre notifica de algo. De esta forma, los datos se pueden usar como base para que un informe de auditoría muestre que un host aprobó o no aprobó una prueba específica, o que no se pudo probar adecuadamente.

Tecnología requerida

Plugins .nbin de Nessus para compatibilidad de configuración de Unix y Windows

Tenable ha creado dos plugins de Nessus (Identificaciones 21156 y 21157) que implementan las API usadas para realizar auditorías en sistemas Unix y Windows. Los plugins se compilaron previamente con el formato “**.nbin**” de Nessus.

Estos plugins y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales y usuarios de SecurityCenter. Este documento también aborda dos herramientas de Windows para ayudar a crear archivos **.audit** personalizados de Windows y una herramienta de Unix para crear archivos **.audit** de Unix.

Para las auditorías de compatibilidad de Unix, solo se admite autenticación SSH. Los protocolos heredados como Telnet no están autorizados por razones de seguridad.

Plugins .nbin de Nessus para compatibilidad de contenido de Windows

Tenable ha creado un plugin de Nessus (Identificación 24760) denominado “Windows File Contents Compliance Checks” (Comprobaciones de compatibilidad de contenido de archivos de Windows) que implementa las API usadas para auditar sistemas de Windows en busca de contenido no compatible, tal como Personally Identifiable Information, PII (Información de identificación personal) o Protected Health Information, PHI (Información médica protegida). Los plugins se compilaron previamente con el formato “**.nbin**” de Nessus. Los plugins y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales y usuarios de SecurityCenter.

Tenga en cuenta que los sistemas Unix no son analizados por el plugin 24760.

Plugin .nbin de Nessus para compatibilidad de bases de datos

Tenable ha creado un plugin de Nessus (Identificación 33814) denominado “Database Compliance Checks” (Comprobaciones de compatibilidad de bases de datos) que implementa las API usadas para auditar distintos sistemas de bases de datos. El plugin se compiló previamente con el formato “**.nbin**” de Nessus. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales y usuarios de SecurityCenter.

Las comprobaciones de compatibilidad de bases de datos no se encuentran disponibles para la versión 3.4.3 de Security Center y anteriores.

Plugin .nbin de Nessus para compatibilidad de IBM iSeries

Tenable ha creado un plugin de Nessus (Identificación 57860) denominado “IBM iSeries Compliance Checks” (Comprobaciones de compatibilidad de IBM iSeries) que implementa las API usadas para auditar sistemas con IBM iSeries. Este plugin se compiló previamente con el formato “**.nbin**” de Nessus. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales.

Para llevar a cabo un análisis de compatibilidad satisfactorio en un sistema iSeries, los usuarios autenticados deben tener los siguientes privilegios:

1. Un usuario con autoridad (*ALLOBJ) o de auditoría (*AUDIT) puede auditar todos los valores del sistema. Este usuario suele pertenecer a la clase (*SECOFR).

2. Los usuarios de clase (*USER) o (*SYSOPR) pueden auditar la mayoría de los valores, excepto QAUDCTL, QAUDENDACN, QAUDFRCLVL, QAUDLVL, QAUDLVL2 y QCRTOBJAUD.

Si un usuario no tiene privilegios para acceder a un valor, el valor regresado será *NOTAVL.

Plugin .nbin de Nessus para compatibilidad de Cisco

Tenable ha creado un plugin de Nessus (Identificación 46689) denominado “Cisco IOS Compliance Checks” (Comprobaciones de compatibilidad de Cisco IOS) que implementa las API usadas para auditar sistemas que ejecutan el sistema operativo CISCO IOS. Este plugin se compiló previamente con el formato “**.nbin**” de Nessus. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales. Esta comprobación de compatibilidad se puede ejecutar en una configuración Saved (Guardada), Running (En ejecución) o Startup (Inicio).

Plugin .nbin de Nessus para Palo Alto

Tenable ha creado un plugin de Nessus (Identificación 64095) denominado “Palo Alto Networks PAN-OS Compliance Checks” (Comprobaciones de compatibilidad de Palo Alto Networks PAN-OS) que implementa las API usadas para auditar sistemas que ejecutan dispositivos Palo Alto. Además, se utiliza un plugin de Nessus (identificación 64286) denominado “Palo Alto Networks Settings” (Configuración de Palo Alto Networks) a fin de configurar la información de autenticación necesaria para realizar la auditoría. Estos plugins se compilaron previamente con el formato “**.nbin**” de Nessus. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales. Esta comprobación de compatibilidad se puede ejecutar con configuraciones operativas.

Plugin .nbin de Nessus para VMware

Tenable ha creado un plugin de Nessus (Identificación 64455) denominado “VMware vCenter/vSphere Compliance Checks” (Comprobaciones de compatibilidad de vCenter/vSphere de VMware) que implementa la API SOAP de VMware para auditar software ESX, ESXi y vCenter. Se puede agregar información de credenciales para realizar una auditoría a las “VMware vCenter SOAP API Settings” (Opciones de configuración de API SOAP de vCenter de VMware) en la sección “Advanced” (Avanzada) de una directiva. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales. Para obtener más información sobre hacer una auditoría en VMware, consulte el artículo de blog asociado.

Plugin .nbin de Nessus para Citrix XenServer

Tenable ha creado un plugin de Nessus (Identificación 69512) denominado “Citrix XenServer Compliance Checks” (Comprobaciones de compatibilidad de Citrix XenServer) que implementa las API usadas para auditar sistemas que ejecutan Citrix XenServer, así como también proveedores que crean sus propias versiones de XenServer según el código abierto. Se puede agregar información de credenciales para realizar una auditoría a “Citrix XenServer Compliance Checks” (Comprobaciones de compatibilidad de Citrix XenServer) en la sección “Advanced” (Avanzada) de una directiva. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales. Para más información sobre hacer una auditoría en XenServer, consulte el artículo de blog asociado.

Plugin .nbin de Nessus para HP ProCurve

Tenable ha creado un plugin de Nessus (Identificación 70271) denominado “HP ProCurve Compliance Checks” (Comprobaciones de compatibilidad de HP ProCurve) que implementa las API usadas para auditar sistemas con ProCurve de HP. Se puede agregar información de credenciales para realizar una auditoría a las preferencias de “HP ProCurve Compliance Checks” (Comprobaciones de compatibilidad de HP ProCurve) en la sección “Advanced”

(Avanzada) de una directiva. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales.

Plugin .nbin de Nessus para FireEye

Tenable ha creado un plugin de Nessus (Identificación 70469) denominado “FireEye Compliance Checks” (Comprobaciones de compatibilidad de FireEye) que implementa las API usadas para auditar sistemas con FireEye. Se puede agregar información de credenciales para realizar una auditoría a las preferencias de “FireEye Compliance Checks” (Comprobaciones de compatibilidad de FireEye) en la sección “Advanced” (Avanzada) de una directiva. El plugin y las correspondientes directivas de auditoría se encuentran disponibles para clientes comerciales.

Directivas de auditoría

Tenable desarrolló una cantidad de distintas directivas de auditoría para plataformas Unix, Windows, Palo Alto, IBM iSeries, VMware y Cisco. Estas se encuentran disponibles como archivos de texto **`.audit`** para suscriptores comerciales y se pueden descargar desde el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/. Para conocer las últimas noticias sobre la funcionalidad de auditoría de Tenable y todas las versiones de archivos **`.audit`** más recientes, consulte los Discussion Forums (Foros de debate): https://discussions.nessus.org/.

Al desarrollar estas directivas de auditoría se tuvieron en cuenta muchos aspectos de las auditorías de compatibilidad comunes, tales como los requisitos de SOX, FISMA y PCI DSS; sin embargo, en el caso de estos criterios, no se representan como archivos de auditoría oficiales. Recomendamos que los usuarios revisen estas directivas **`.audit`** y personalicen estas comprobaciones en función de su entorno local. Los usuarios pueden cambiar el nombre de los archivos **`.audit`** para adaptarlos a las descripciones locales. Otras directivas **`.audit`** provienen directamente de parámetros de configuración recomendados por CERT, CIS, NSA y NIST.

Tenable espera crear varios tipos diferentes de archivos **`.audit`** de acuerdo con los comentarios de los clientes y con los cambios en las “prácticas recomendadas”. Varias organizaciones de consultoría y los clientes de Tenable también han comenzado a implementar sus propias directivas **`.audit`** y han expresado su interés por compartirlas con otros usuarios comerciales de Nessus. A través de los Tenable Network Security Discussion Forums (Foros de debate de seguridad de redes de Tenable) en https://discussions.nessus.org/, se puede obtener una forma sencilla de compartir directivas **`.audit`** o simplemente interactuar con la comunidad de Nessus.

Utilidades de ayuda

Tenable ha desarrollado una herramienta que convierte archivos **`.inf`** en archivos **`.audit`** de Nessus para realizar auditorías de Windows. Esta herramienta se denomina **`i2a`**, y también se aborda posteriormente en este documento.

Existen dos herramientas de Unix que se pueden usar para crear archivos **`.audit`** de Unix. La primera herramienta, denominada **`c2a`** (que significa “configuration to audit” [configuración para auditar]), se puede usar para crear archivos **`.audit`** de Unix directamente a partir de archivos de configuración existentes. Por ejemplo, si su archivo de configuración Sendmail está configurado correctamente de acuerdo con la directiva de su sitio, la herramienta **`c2a`** puede crear una directiva de auditoría en función de la suma de comprobación MD5 del archivo o de acuerdo con pares de valores y argumentos específicos en el archivo **`sendmail.cf`**. La segunda herramienta, denominada **`p2a`** (que significa “package to audit” [paquete para auditar]), puede usarse para crear archivos **`.audit`** de Unix a partir del conjunto de paquetes base en un sistema Unix (Solaris 10 o Linux basado en RPM) o a partir de un archivo de texto sin formato con una lista de nombres de paquetes.

Analizadores Nessus para Unix o Windows

Para ejecutar comprobaciones de compatibilidad se puede usar una variedad de plataformas, y generalmente el sistema operativo subyacente en el que resida Nessus no reviste importancia. Usted puede realizar auditorías de compatibilidad de servidores de Windows 2003 desde un equipo portátil con OS X y también puede auditar servidores Solaris desde un equipo portátil con Windows.

Credenciales para dispositivos que se auditarán

En todos los casos se necesitan credenciales de Unix SSH, dominio de Windows, IBM iSeries, Cisco IOS o bases de datos para que Nessus inicie sesión en los servidores de destino. En la mayoría de las ocasiones, este usuario debe ser un “Super user” (superusuario) o un usuario habitual con capacidad de escalada de privilegios (por ejemplo, **`sudo`**, **`su`** o

su+sudo). Si el usuario que realiza la auditoría no tiene privilegios de “Super user” (superusuario), muchos de los comandos del sistema remoto no se podrán ejecutar, o bien devolverán resultados incorrectos.

La cuenta de Windows usada para las credenciales de inicio de sesión debe tener permiso para leer la directiva del equipo local. Si un host de destino no forma parte de un dominio de Windows, la cuenta debe ser miembro del grupo de administradores del host. Si el host participa en un dominio, el grupo de administradores del dominio será miembro del grupo de administradores del host, y la cuenta tendrá acceso a la directiva de equipo local si es miembro del grupo de administradores del dominio.

Para realizar comprobaciones de compatibilidad de contenido de Windows, además de iniciar sesión en el sistema con privilegios de dominio, debe permitirse el acceso al Windows Management Instrumentation, WMI (Instrumental de administración de Windows). Si el acceso no se encuentra disponible, Nessus indicará que no se pudo obtener acceso a WMI para realizar el análisis.

Las comprobaciones de compatibilidad de bases de datos solo requieren credenciales de bases de datos para llevar a cabo una auditoría completa de compatibilidad. Esto se debe a que es la base de datos, y no el sistema operativo host, lo que se está analizando para determinar la compatibilidad.

Las comprobaciones de compatibilidad de Cisco IOS normalmente requieren la contraseña “enable” (habilitar) para realizar una auditoría completa de compatibilidad de la configuración del sistema. El motivo es que Nessus efectúa una auditoría de los resultados generados por el comando “**show config**”, que solo están disponibles para los usuarios con privilegios. Si el usuario de Nessus que se emplea para la auditoría ya posee privilegios “enable” (habilitar), no es necesaria la contraseña “enable” (habilitar).

Para obtener más información sobre cómo configurar Nessus o SecurityCenter a fin de realizar comprobaciones de vulnerabilidades con credenciales locales, consulte el documento “Nessus Credentials Checks for Unix and Windows” (“Comprobaciones con credenciales de Nessus para Unix y Windows”), que puede encontrar en http://www.tenable.com/products/nessus/documentation.

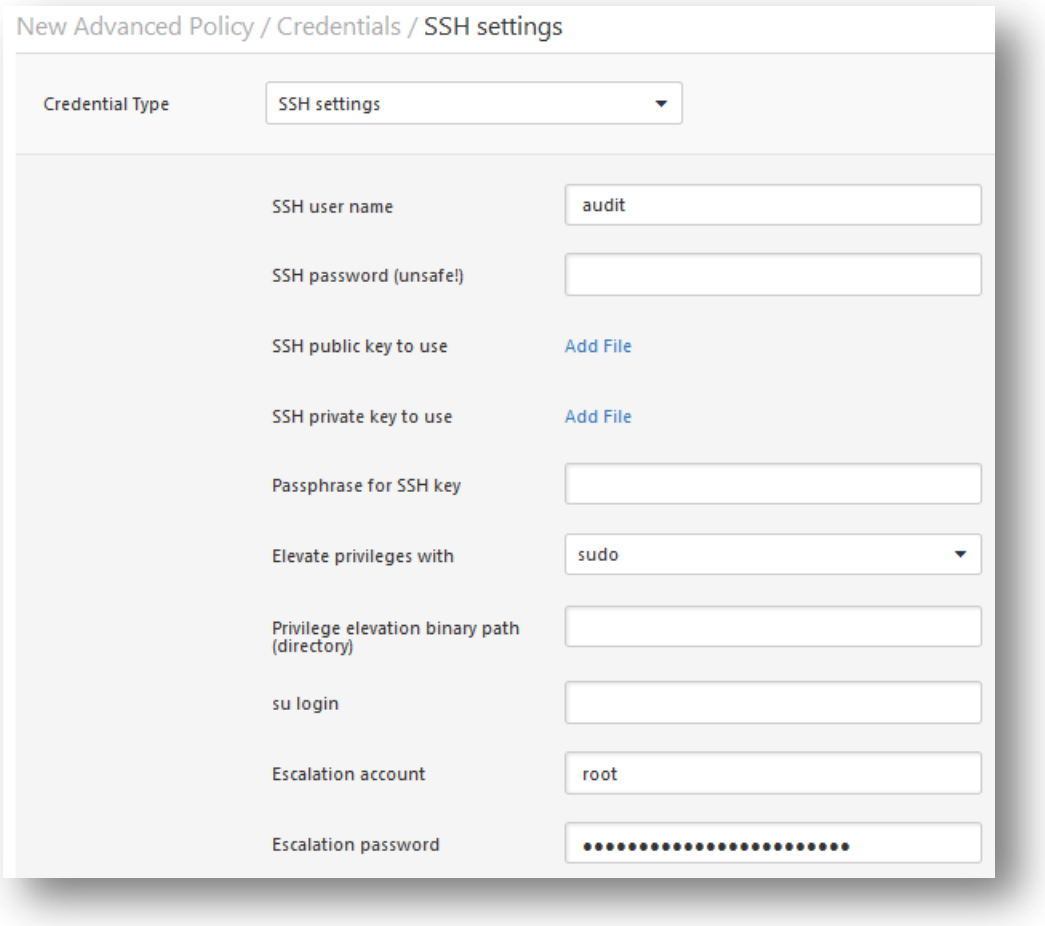
Uso de “su”, “sudo” y “su+sudo” en auditorías

Use “**su+sudo**” en los casos en que la política de la empresa prohíba que Nessus inicie sesión en un host remoto con el usuario root o un usuario con privilegios “**sudo**”. Al realizar un inicio de sesión remoto, el usuario Nessus sin privilegios puede “**su**” (cambiar usuario) por un usuario con privilegios **sudo**.

Los análisis con credenciales en Unix más eficaces son aquellos que se realizan cuando las credenciales proporcionadas tienen privilegios “root” (raíz). Dado que muchos sitios no permiten un inicio de sesión remoto como root (raíz), los usuarios de Nessus pueden ahora invocar “**su**”, “**sudo**” o “**su+sudo**” con una contraseña separada para una cuenta que se haya configurado para que tenga los privilegios apropiados.

Además, 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. Esta acción le garantiza que el 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.

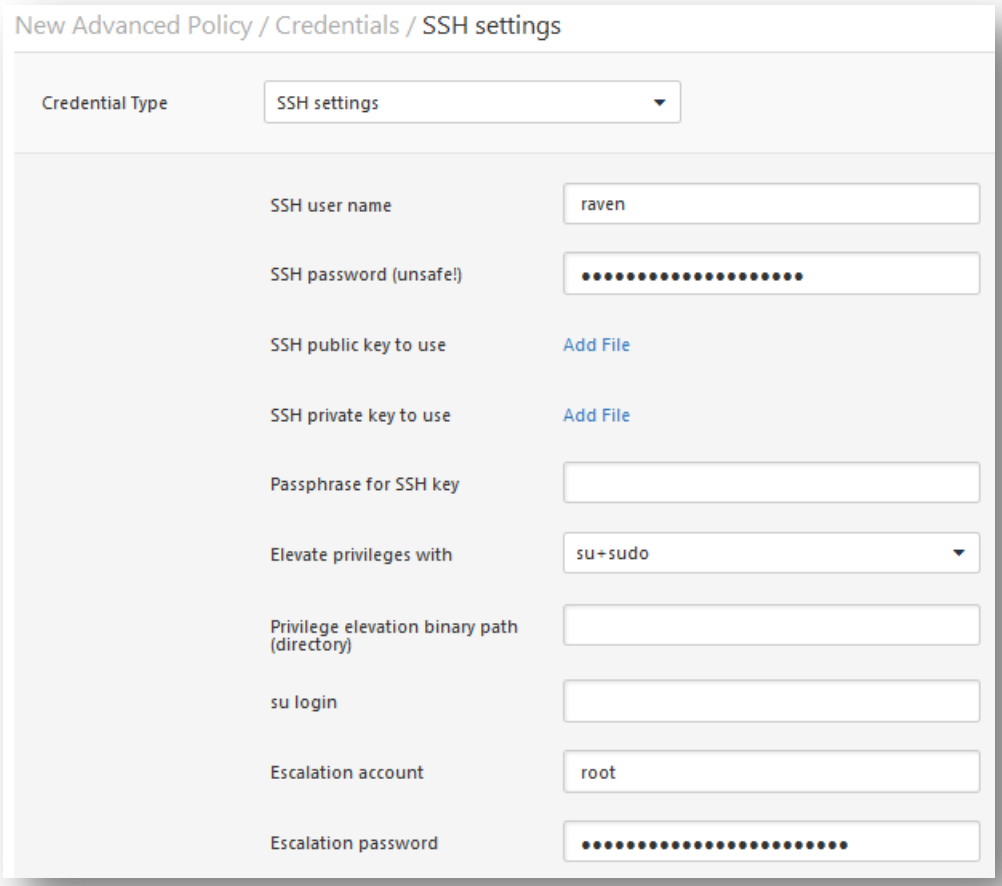
Ejemplo de sudo
A continuación se presenta un ejemplo de captura de pantalla del uso de "**sudo**" junto con las claves de SSH. A los fines de este ejemplo, la cuenta de usuario es "audit" (auditoría), que se ha añadido al archivo **/etc/sudoers** en el sistema que se analizará. La contraseña proporcionada 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):



Ejemplo de su+sudo
En la versión Nessus 4.2.2 se incluyó un nuevo método de elevación de credenciales para hosts basados en Unix que tengan instalado **sudo**: "**su+sudo**". Este método le permite asignar credenciales a una cuenta que no tenga permisos **sudo**, **su** (cambiar usuario) a una cuenta de usuario que sí los tenga, y luego emitir el comando **sudo**.

Esta configuración brinda mayor seguridad para sus credenciales durante el análisis y cumple con los requisitos de compatibilidad de muchas organizaciones.

Para habilitar esta característica, simplemente seleccione “su+sudo” en la sección “Elevate privileges with” (Elevar privilegios con) de la configuración de credenciales/SSH, como se muestra en la siguiente captura de pantalla:



En los campos “SSH user name” (Nombre de usuario SSH) y “SSH password” (Contraseña SSH), introduzca las credenciales que no cuentan con privilegios **`sudo`**. En el ejemplo anterior, la cuenta de usuario es “raven”. Desde el menú desplegable “Elevate privileges with” (Elevar privilegios con), seleccione “su+sudo”. En los campos “su login” (Inicio de sesión su) y “Escalation password” (Contraseña de escalación), introduzca el nombre de usuario y contraseña que *sí* poseen credenciales con privilegios. En este ejemplo: “sumi”. No es necesario ningún otro cambio en la directiva de análisis.

Consideración importante respecto de sudo
Al realizar auditorías en sistemas Unix mediante **`su`**, **`sudo`** o **`su+sudo`**, tenga en cuenta los siguientes puntos:

- Si su sistema Unix fue protegido para limitar qué comandos se pueden ejecutar mediante **`sudo`** o archivos a los que tienen acceso usuarios remotos, esto puede afectar su auditoría. Compare las auditorías que no sean root con una auditoría root si sospecha que la auditoría se ve limitada por medidas de seguridad.

- El comando **`sudo`** no es nativo de Solaris, y necesita descargarse e instalarse si su sistema de destino ejecuta Solaris. Asegúrese de que se pueda obtener acceso al binario **`sudo`** como “**`/usr/bin/sudo`**”.

- Cuando se analiza mediante **`known_hosts`**, el análisis de Nessus aún necesita especificar también un host para analizar. Por ejemplo, si analizó una clase C pero cargó un archivo **`known_hosts`** que solo contenía 20 hosts individuales dentro de esa clase C, Nessus solo analizaría esos hosts del archivo.

- Algunas configuraciones basadas en Unix requieren que los comandos iniciados por sudo se ejecuten a partir de sesiones **tty**. Los análisis de vulnerabilidades de Nessus realizados mediante la opción "**su+sudo**" no cumplen con ese requisito. Si usa la opción "**su+sudo**", deberá crear una excepción en el sistema de destino. Para determinar si este es el caso para su distribución de Unix, introduzca el siguiente comando como root (raíz) en el sistema que analizará:

  ```
  # grep requiretty `locate sudoers` | grep -v "#" | grep /etc
  ```

  Si la línea "**requiretty**" se encuentra en el archivo de configuración **sudoers**, será necesario crear una excepción a esta regla en el archivo **/etc/sudoers** de la siguiente manera:

  ```
  Defaults requiretty
  Defaults:{userid} !requiretty
  ```

  Tenga en cuenta que {userid} es el nombre de usuario que se empleará para ejecutar el comando "**sudo**" (la página "su login" [Inicio de sesión su] en la sección de credenciales/SSH de su directiva). También asegúrese de contar con la siguiente línea en su archivo **sudoers**:

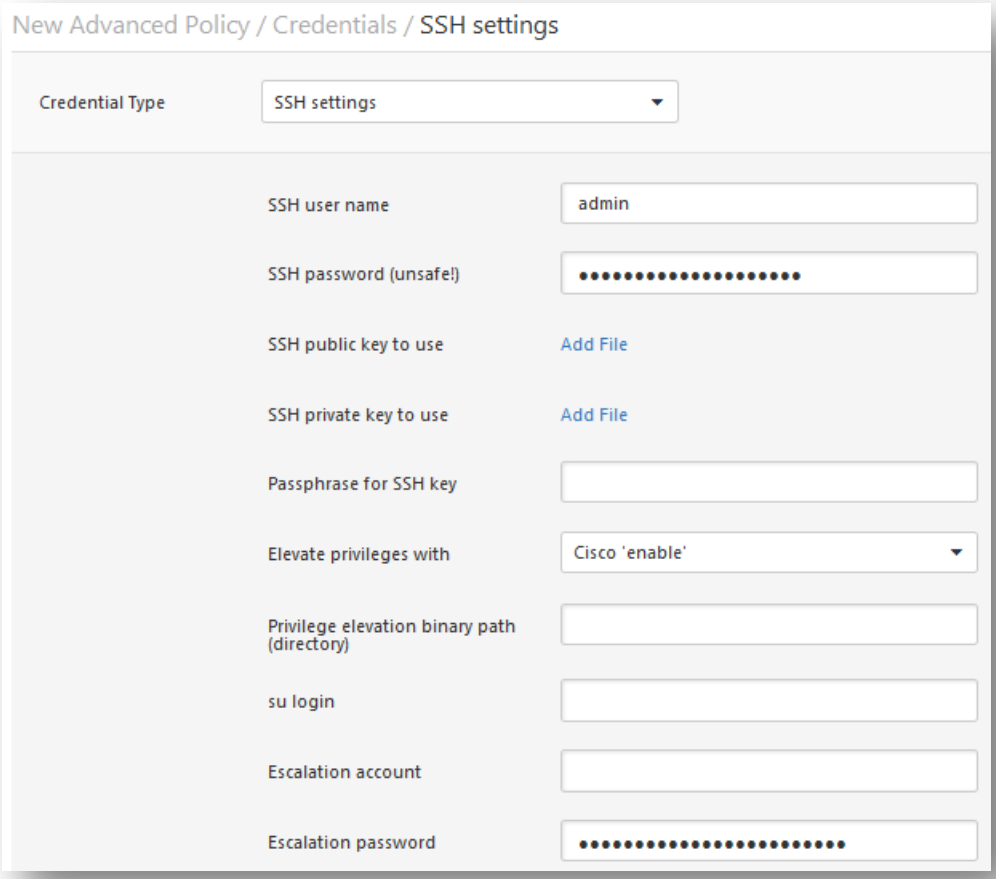
  ```
  {userid} ALL=(ALL) ALL
  ```

  Tenga en cuenta que nuevamente {userid} es el nombre de usuario que se empleará para ejecutar el comando "**sudo**" (el "su login" [Inicio de sesión su] en la sección de credenciales/SSH de su directiva).

Ejemplo de Cisco IOS:

Solo se admite la autenticación SSH. Los dispositivos IOS heredados que requieren Telnet para realizar la autenticación no pueden analizarse mediante las comprobaciones de compatibilidad de Cisco que realiza Nessus.

Las credenciales de Cisco IOS se configuran mediante la pantalla de credenciales "**SSH settings**" (Configuración de SSH) en la interfaz de usuario de Nessus. Introduzca el nombre de usuario y contraseña de SSH necesarios para iniciar sesión en el enrutador de Cisco. Para especificar que los privilegios deben elevarse con "Enable" (Habilitar), elija "**Cisco 'enable'**" ('Habilitar' de Cisco) junto a la opción "**Elevate privileges with**" (Elevar privilegios con) e introduzca la contraseña de habilitación junto a "**Escalation password**" (Contraseña de escalación).



Conversión de archivos .inf de Windows en archivos .audit con i2a

Si usted o su organización de TI posee archivos de directivas de Windows (normalmente se encuentran con la extensión "**.inf**"), los mismos se pueden convertir en archivos **.audit** para usar en auditorías de Nessus en servidores de Windows.

Obtención e instalación de la herramienta

La herramienta **i2a** se encuentra disponible como archivo zip y se puede obtener en el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/. Esta herramienta no usa una GUI, y se ejecuta desde la línea de comandos.

Extraiga el contenido del archivo en un directorio de su elección, y luego mueva sus archivos **.inf** de Windows al mismo directorio.

Conversión de archivos .inf en .audit

Ejecute la herramienta de conversión desde el símbolo del sistema, simplemente escribiendo:

```
# i2a-x.x.x.exe yourfile.inf file.audit
```

En este ejemplo, **yourfile.inf** es el archivo **.inf** de origen y **file.audit** es el archivo **.audit** de destino.

Análisis de la conversión

Tenable intentó lograr una conversión casi al 100% entre lo que se puede describir en los archivos **.inf** y lo que se puede auditar en los archivos **.audit**. No obstante, hay algunos elementos de directivas que no se pueden probar con la actual tecnología Nessus 5.

Para cada ejecución de la herramienta **i2a** se crea un registro del proceso de conversión. Contiene una auditoría línea por línea de todo el proceso de conversión. Si una línea del **.inf** no se puede convertir, aparecerá en este archivo de registro.

Formato correcto de vonfiguración de .inf

En el caso de las comprobaciones que aparecen en el archivo de registro y que no se pudieron procesar, asegúrese de que cumplan con los formatos aceptados que se indican a continuación.

Las opciones **System Access** (Acceso al sistema), **System Log** (Registro del sistema), **Security Log** (Registro de seguridad), **Application Log** (Registro de aplicaciones) y **Event Audit** (Auditoría de eventos) comparten el mismo formato. Cada entrada es descrita por la "**Key**" (clave), seguida por un "**value**" (valor).

Sintaxis:

```
Key = value
```

En el caso anterior, "**Key**" es el elemento que se auditará y "**value**" es el valor esperado para esa clave en el sistema remoto.

Ejemplo:

```
MinimumPasswordLength = 8
```

El formato de las opciones de **Privilege Rights** (Derechos de privilegio) es similar al mencionado anteriormente. Sin embargo, en esta opción el valor puede quedar vacío.

Sintaxis:

```
PriviledgeRight = User1,User2…UserN
```

Ejemplo:

```
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-544
```

O bien:

```
SeTcbPrivilege =
```

Una opción de **Registry Key** (Clave de registro) consiste en las siguientes cuatro partes:

- Registry Key (Clave de registro): la clave de registro que se debe auditar.
- Inheritance Value (Valor heredado): identifica si los permisos para la clave de registro son heredados o no heredados. El valor puede ser [0-4].
- DACL: DACL es una ACL que es controlada por el propietario de un objeto, y especifica el acceso al objeto que pueden tener usuarios particulares o grupos específicos.

- SACL: SACL es una ACL que controla la generación de mensajes de auditoría correspondientes a los intentos de acceder a un objeto protegible.

Sintaxis:

```
"Registry Key",Inheritance value,
"D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)... (string_acen)"
```

Los campos DACL y SACL pueden estar vacíos, en cuyo caso la comprobación se omitirá.

Ejemplo:

```
"MACHINE\SYSTEM\CurrentControlSet\Control\Class",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)
      S:PAR(AU;OICIFA;CC;;;WD)"
```

El formato de la opción **File Security** (Seguridad del archivo) es similar al formato de la Clave de registro que se describió anteriormente.

Sintaxis:

```
"File Object",Inheritance value,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...
      (string_acen)"
```

Ejemplo:

```
"%SystemRoot%\system32\ciadv.msc",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICI
      FA;CC;;;WD)"
```

La opción **Service General** (General de servicio) consiste en las siguientes cuatro partes:

- Service Name (Nombre del servicio): el servicio que se debe auditar.
- Service start type (Tipo de inicio del servicio): Manual (Manual), Automatic (Automático) o Disabled (Deshabilitado). El valor puede ser [2-4].
- DACL: DACL es una ACL que es controlada por el propietario de un objeto, y especifica el acceso al objeto que pueden tener usuarios particulares o grupos específicos.
- SACL: SACL es una ACL que controla la generación de mensajes de auditoría correspondientes a los intentos de acceder a un objeto protegible.

Sintaxis:

```
Service Name,Start type,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...(string_a
      cen)"
```

Ejemplo:

```
kdc,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLO
```

```
        CRRC;;;SY)"
```

Si no se deben comprobar los permisos para una opción de servicio y solo se debe auditar el tipo de inicio, esto se puede realizar de la siguiente forma:

Sintaxis:

```
Service Name,Start type
```

Ejemplo:

```
kdc,3,""
```

La opción **Registry Value** (Valores de registro) consiste en las siguientes tres partes:

- RegistryKey: la clave de registro que se debe auditar.
- RegistryType: el tipo de registro (REG_DWORD, REG_SZ, etc.).
- RegistryValue: el valor correspondiente a la clave de registro.

RegistryValue puede definirse entre comillas dobles, comillas simples o sin comillas.

Sintaxis:

```
RegistryKey,RegistryType,RegistryValue
```

Ejemplo:

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
```

Si desea comentar una línea en particular dentro del archivo **`.inf`**, anexe un punto y coma ";" delante de la línea, y la secuencia de comandos omitirá esa línea.

Conversión de archivos de configuración de Unix en archivos .audit con c2a

La herramienta **`c2a.pl`** está diseñada para asistir a los auditores en la creación de archivos **`.audit`** para auditar las configuraciones de aplicaciones de una red en particular. Por ejemplo, si desea que todos los servidores web de una red en particular estén configurados exactamente como el host maestro X, debería ejecutar esta herramienta en el host X, crear el archivo **`.audit`** para **`httpd`** en ese sistema, y luego introducir este archivo en el demonio de Nessus y ejecutar el análisis en todos los otros servidores web para comprobar la compatibilidad.

De manera opcional, esta herramienta se puede usar también para crear archivos de auditoría MD5 para un host completo. La herramienta espera una lista de archivos/directorios que se debe auditar en un archivo de entrada, que luego procesará de manera recursiva en el caso de los directorios, con el fin de crear un archivo **`.audit`** para el sistema. Posteriormente, este archivo se puede usar para analizar los cambios en los archivos y los directorios principales.

Obtención e instalación de la herramienta

La herramienta **c2a** es un archivo **tar** comprimido que se puede obtener en el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/.

Extraiga el contenido de **c2a-x.x.x.tar.gz** en su equipo local mediante el siguiente comando:

```
# tar xzf c2a-x.x.x.tar.gz
```

De esta forma, se creará un directorio "**c2a**" en el directorio actual y se extraerán los archivos en él. Si desea extraer el contenido en un directorio que elija, use el siguiente comando:

```
# tar xzf c2a.x.x.x.tar.gz –C /path/to/directory
```

Después de descomprimir el archivo, deberá ver los siguientes archivos en el directorio **~/c2a**:

- **c2a.pl**
- **c2a.map**
- **c2a_regex.map**
- **cmv.pl**
- **ReadMe.txt**

Creación de un archivo de auditoría MD5

Ejecute la herramienta de conversión con la opción "**-md5**" escribiendo:

```
# ./c2a.pl -md5 -f /path/to/inputfile.txt -o outputfile.audit
```

La herramienta espera un archivo de entrada con una lista de archivos y directorios que deben auditarse en busca de valores MD5, así como un nombre de archivo de salida correspondiente al archivo de auditoría.

Al añadir archivos a su archivo de entrada, recuerde usar este formato:

`/path/to/file`

Use este formato al añadir directorios:

`/path/to/file/`

Si se usa este formato y el archivo es efectivamente un archivo y no un directorio, la herramienta `c2a` indicará que este archivo no existe. La barra inicial "/" es totalmente adecuada para agregar directorios.

Si la entrada del archivo de entrada es un archivo MD5 normal, solo se calculará ese archivo y se escribirá en el formato **.audit**. En el caso de un directorio, la secuencia de comandos hurgará de manera recursiva en todos y cada uno de los archivos de ese directorio. Si no se especifica un archivo de salida, el resultado se incluirá en **~/c2a/op.audit**.

Al procesar la lista de archivos especificados por "inputfile", se omitirá cualquier enlace simbólico que se encuentre. Aparecerá un mensaje de advertencia que indicará que el archivo no existe o se trata de un enlace simbólico. A partir de esta versión, **c2a** no admite enlaces simbólicos.

Creación de un archivo de auditoría en función de uno o más archivos de configuración

La herramienta **c2a** resulta ideal para procesar archivos de configuración que poseen contenido línea por línea exclusivo. Si su archivo de configuración tiene funciones multilínea, por ejemplo, un archivo de configuración XML, **c2a** no es una buena opción.

Ejecute la herramienta de conversión con la opción "**-audit**" escribiendo:

```
# ./c2a.pl -audit -f /path/to/input.txt -o outputfile.audit
```

La herramienta espera un archivo de entrada (**input.txt**) que contenga una lista de los archivos de configuración que deban auditarse, así como un nombre de archivo de salida correspondiente al archivo de auditoría.

La secuencia de comandos de Perl **c2a.pl** se basa sobre dos archivos de claves: **c2a.map** y **c2a_regex.map**. Analiza cada línea del archivo de configuración que se está auditando y comprueba si la primera palabra de esa línea coincide con el "tipo" en el archivo **c2a.map** (por ejemplo, HTTP, SENDMAIL, etc.), y el valor que se encuentra asociado a este. Por ejemplo, si está realizando una auditoría de configuración HTTP, comprueba si la palabra coincide con alguna de las palabras clave HTTP en el archivo **c2a.map**. Si coincide, aplica la expresión regex de **c2a_regex.map** para HTTP en esa línea y extrae la opción y el valor. Solo se auditará la configuración para la cual exista una entrada en **c2a.map**.

Los archivos de configuración que no se desea auditar se pueden comentar mediante el carácter "**#**".

Si desea convertir a formato **.audit** a las opciones que fueron comentadas en el archivo de configuración, modifique el **c2a.pl** y establezca `$ENFORCE_COMMENT = 1;`".

Como en el caso anterior, si no se especifica el archivo de salida, el resultado se incluirá en **~/c2a/op.audit**.

Actualmente, Tenable proporciona configuración MAP para HTTP, SENDMAIL, SYSCTL y NESSUS. Se pueden añadir fácilmente opciones para aplicaciones adicionales mediante la secuencia de comandos de Perl **cmv.pl**. Consulte la siguiente sección para obtener más información.

Creación de un archivo MAP

Crear un archivo MAP para una aplicación es simple. Solo ejecute la secuencia de comandos **cmv.pl** de la siguiente forma:

```
# ./cmv.pl -r 'regex' -r tag -f config_file
```

Donde:

- "**regex**" representa la regex para extraer el par de valores y opción de configuración. Normalmente tiene la forma "<name> = <value>". Pero en algunos casos podría ser ligeramente diferente; en ellos, "=" podría ser reemplazado por un espacio, una tabulación, etc.
- "**tag**" es esencialmente la palabra clave con la que usted desea etiquetar la aplicación que está siendo auditada. La palabra clave **tag** vincula el **config_file** con las palabras claves de **c2a.map** y el regex de **c2a_regex.map**; por lo tanto, es importante que la etiqueta de cada uno de estos archivos sea la misma.
- "**config_file**" es el archivo para el que se crea un archivo MAP.

Por ejemplo, si desea auditar opciones de configuración de VSFTPD, siga estos pasos:

1. Primero use **cmv.pl** de la siguiente forma:

   ```
   # ./cmv.pl -r '([A-Za-z0-9_]+)=([A-Za-z0-9]+)' -t VSFTPD -f /root/vsftpd-0.9.2/vsftpd.conf
   ```

   Esto creará el archivo **tag.map** (por ejemplo, **VSFTPD.map**). De manera predeterminada, todas las líneas con comentarios se omitirán. Si desea tener en cuenta todas las variables, cambie el valor **$ENFORCE_COMMENT** de "0" a "1" y luego vuelva a ejecutar la secuencia de comandos.

2. Inspeccione y anexe el archivo MAP a **c2a.map**.

   Revise el archivo **VSFTPD.map** en busca de valores no deseados que pudieran haber coincidido inesperadamente con su expresión regex. Después de examinar y determinar que todas las palabras claves sean correctas, anéxelas a **c2a.map**.

3. Actualice **c2a_regex.map** con la misma expresión usada por **cmv.pl**, de la siguiente forma:

   ```
   VSFTPD=([A-Za-z0-9_]+)=([A-Za-z0-9]+)
   ```

   Nota: es la misma expresión regex que la usada por la secuencia de comandos de Perl **cmv.pl**.

4. Actualice **input.txt** con la ubicación del archivo de configuración VSFTPD:

   ```
   VSFTPD=/root/vsftpd-0.9.2/vsftpd.conf
   ```

5. Ejecute la secuencia de comandos **c2a.pl**:

   ```
   # ./c2a.pl -audit -f input.txt
   ```

6. Por último, revise el archivo de salida:

   ```
   # vi op.audit
   ```

Otros usos de la herramienta c2a

Tenable ha incluido varias entradas en los archivos **c2a.map** y **c2a_regex.map** para habilitar la auditoría de Sendmail, el Very Secure FTP Daemon (VSFTPD), Apache, el archivo **/etc/sysctl.conf** de Red Hat, y Nessus. En el futuro próximo, es posible que se añada más software. Si desea presentar nuevas asignaciones a Tenable para compartirlas con otros usuarios de Nessus, envíelas a nessus-support@tenable.com.

Teniendo eso en cuenta, la secuencia de comandos **c2a.pl** se puede usar a fin de crear archivos **.audit** de Nessus para varias aplicaciones activas de Unix. Considere las siguientes ideas:

- Si su organización posee muchos firewalls basados en Unix, se puede generar un archivo **.audit** para auditar las opciones habituales y obligatorias con las que se supone que debe contar todo firewall. Por ejemplo, si todos los firewalls debieran tener filtros de direcciones RFC 1918, se pueden probar las reglas reales de los firewalls.

- Si se ejecutan desde CRON muchas aplicaciones personalizadas diferentes, se pueden auditar los distintos CRONTABs para verificar que se estén ejecutando las aplicaciones adecuadas en el momento correcto.

- Para un inicio de sesión centralizado, se pueden comprobar las configuraciones SYSLOG, SYSLOG-NG y LOGROTATE de los sistemas Unix remotos.

Ajuste manual de los archivos .audit

Por último, los resultados de la secuencia de comandos **c2a.pl** también se pueden modificar de forma manual. Por ejemplo, considere la combinación de las reglas de suma de comprobación MD5 con las reglas de FILE_CONTENT_CHECK en una sola. Los resultados generados por la secuencia de comandos **c2a.pl** también

suponen que un archivo de configuración siempre se encuentra en un solo lugar. Considere la modificación de la palabra clave "**file**" para especificar otras ubicaciones en las que se puede encontrar un archivo de configuración.

Si posee contenido que no desea en sus configuraciones de archivos remotos, considere la posibilidad de añadir manualmente comprobaciones que las verifiquen, con la palabra clave FILE_CONTENT_CHECK_NOT. Esto puede ayudarle a realizar auditorías de las opciones que deben existir, así como de las que no deben existir.

Conversión de listas de paquetes de Unix en archivos .audit con p2a

La herramienta **p2a.pl** está diseñada para asistir a los auditores en la creación de archivos **.audit** para instalar configuraciones de paquetes en sistemas Solaris 10 y Linux basados en RPM. Por ejemplo, si desea que todos los servidores web de Linux de una red en particular tengan la misma base RPM que el host maestro X, debería ejecutar esta herramienta en el host X, lo que crearía un archivo **.audit** con todos los paquetes RPM en ese sistema. Luego debería usar el archivo **.audit** con Nessus para ejecutar un análisis de otros servidores web, para comprobar la compatibilidad.

De manera opcional, esta herramienta se puede usar para crear un archivo de auditoría a partir de una lista de texto de paquetes Solaris 10 o RPM. La herramienta espera una lista de paquetes, uno por línea, en un archivo de entrada, y luego le da el formato correcto a un archivo **.audit** para el sistema objetivo. Posteriormente, el archivo **.audit** generado se puede usar para analizar los cambios en los paquetes de instalación principales.

Obtención e instalación de la herramienta

La herramienta **p2a** es un archivo **tar** comprimido que consta de una única secuencia de comandos de Perl y un archivo de ayuda **ReadMe.txt**. Se puede obtener en el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/.

Extraiga el contenido de **p2a-x.x.x.tar.gz** en su equipo local mediante el siguiente comando:

```
# tar xzf p2a-x.x.x.tar.gz
```

De esta forma, se creará un directorio "**p2a**" en el directorio actual y se extraerán los archivos en este.

Si desea extraer el contenido en un directorio que elija, use el siguiente comando:

```
# tar xzf p2a.x.x.x.tar.gz -C /path/to/directory
```

Después de descomprimir el archivo, deberá ver los siguientes archivos en el directorio **~/p2a**:

- **p2a.pl**
- **ReadMe.txt**

Haga que la secuencia de comandos sea ejecutable mediante la ejecución de:

```
# chmod 750 p2a.pl
```

Uso

Ejecute la secuencia de comandos de Perl de la siguiente forma:

```
# ./p2a.pl [-h] -i inputfile.txt -o outputfile.audit
```

"**-h**" constituye un argumento independiente opcional que muestra la herramienta de ayuda.

Creación de un archivo de salida en función de todos los paquetes instalados

Si la secuencia de comandos se ejecuta únicamente con la opción "**-o**", ejecuta un comando del sistema para extraer todos los nombres de paquetes del sistema instalados localmente, y el archivo **.audit** resultante se incluirá en **/path/to/outputfile.audit**.

```
# ./p2a.pl -o /path/to/outputfile.audit
```

Los archivos de salida deben incluir la extensión **.audit** para que se ejecute la secuencia de comandos. De lo contrario, se generará un error que indicará una extensión de archivo incorrecta.

Creación de un archivo de salida en función de una lista de paquetes y visualización en pantalla

Ejecute **p2a** para enviar todos los resultados obtenidos a la ventana del terminal, con la siguiente sintaxis:

```
# ./p2a.pl -i /path/to/inputfile.txt
```

Esta opción requiere un archivo de entrada y generará resultados en la ventana del terminal (**stdout**) que se pueden copiar y pegar en su archivo **.audit**. Al archivo de entrada se le debe dar formato con un paquete por línea y sin delimitadores añadidos.

Ejemplo:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Dado que muchos sistemas basados en Unix pueden tener instalados más de mil paquetes, la cantidad de resultados puede superar su memoria búfer de desplazamiento, lo cual puede dificultar la visualización de todos los resultados.

Creación de un archivo de auditoría en base a un archivo de entrada especificado

Cuando se ejecuta **p2a** con argumentos de entrada y salida, se toma la lista de paquetes con formato y se genera un archivo **.audit** en la ubicación especificada.

```
# ./p2a.pl -i /path/to/input_file.txt -o /path/to/outputfile.audit
```

A los archivos de entrada se les debe dar formato con un paquete por línea y sin delimitadores añadidos.

Ejemplo:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Los archivos de salida deben incluir la extensión **`.audit`** para que se ejecute la secuencia de comandos. De lo contrario, se generará un error que indicará una extensión de archivo incorrecta.

Ejemplo de uso de la interfaz de usuario de Nessus

Obtención de las comprobaciones de compatibilidad

Los clientes comerciales ya contarán con las comprobaciones de compatibilidad para su analizador Nessus, y varios archivos **`.audit`** se encuentran disponibles en el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/. Para confirmarlo, ejecute la interfaz de usuario de Nessus, realice una autenticación y administre o modifique una directiva existente. En la ficha "Plugins" (Plugins) busque la familia "Policy Compliance" (Compatibilidad con directivas), haga clic en el nombre de la familia de plugins y verifique que aparezcan en pantalla los siguientes plugins:

- Cisco IOS Compliance Checks (Comprobaciones de compatibilidad de Cisco IOS)
- Database Compliance Checks (Comprobaciones de compatibilidad de bases de datos)
- IBM iSeries Compliance Checks (Comprobaciones de compatibilidad de IBM iSeries)
- PCI DSS Compliance (Compatibilidad PCI DSS)
- PCI DSS Compliance: Database Reachable from the Internet (Compatibilidad PCI DSS: la base de datos se puede acceder desde Internet)
- PCI DSS Compliance: Handling False Positives (Compatibilidad PCI DSS: manejo de falsos positivos)
- PCI DSS Compliance: Insecure Communication Has Been Detected (Compatibilidad PCI DSS: se ha detectado una comunicación insegura)
- PCI DSS Compliance: Remote Access Software Has Been Detected (Compatibilidad PCI DSS: se ha detectado software de acceso remoto)
- PCI DSS Compliance: Passed (Compatibilidad PCI DSS: aprobado)
- PCI DSS Compliance: Tests Requirements (Compatibilidad PCI DSS: requisitos de prueba)
- Unix Compliance Checks (Comprobaciones de compatibilidad con Unix)
- Windows Compliance Checks (Comprobaciones de compatibilidad de Windows)
- Windows File Contents Compliance Checks (Comprobaciones de compatibilidad de contenido de archivos de Windows)

Configuración de una directiva de análisis

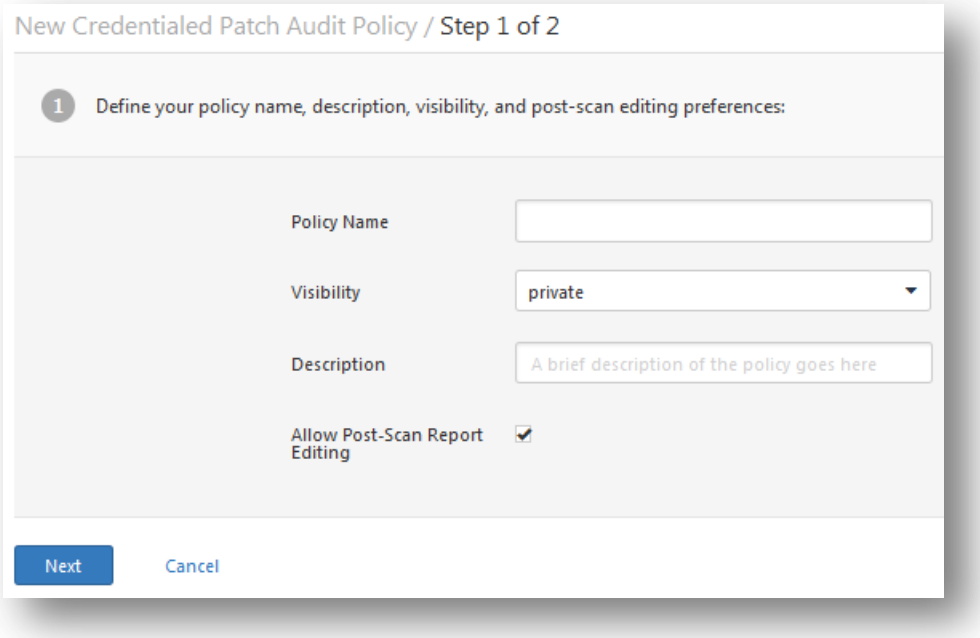
Para habilitar las comprobaciones de compatibilidad en Nessus, se debe crear una directiva de análisis con los siguientes atributos:

- Habilite los plugins de comprobaciones de compatibilidad, que se encuentran en la familia de plugins "Policy Compliance" (Compatibilidad con directivas);
- Especifique como preferencia una o más directivas de compatibilidad **`.audit`**;
- Especifique las credenciales para obtener acceso al servidor de destino, incluidas las credenciales de bases de datos, en la ficha "Preferences" (Preferencias), si corresponde;
- Habilite las dependencias de los plugins.

Esto solo puede hacerse por medio del Policy Wizard (Asistente de directivas) y seleccionando el asistente "**Credentialed Patch Audit**" (Auditoría de revisión con credenciales) o manualmente por medio de "**Advanced Policy**" (Directiva avanzada).

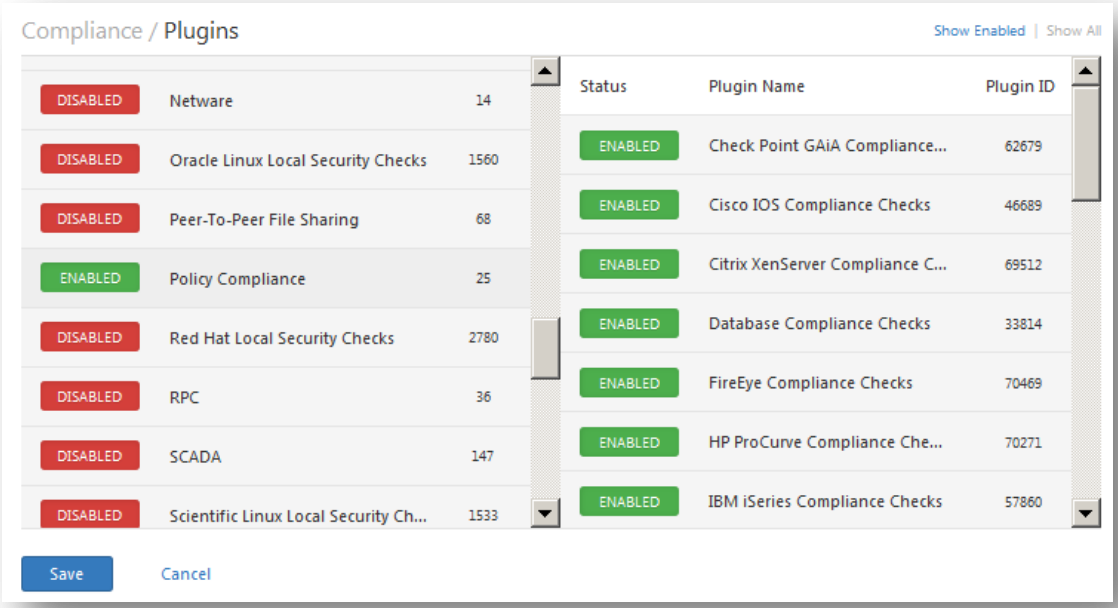
Es importante comprender las comprobaciones en los archivos **`.audit`** que seleccione, especialmente cuando se crearon archivos personalizados. Al usar dos archivos **`.audit`** en el mismo análisis, ambos archivos se combinarán para que los resultados de cada archivo se generen en un único análisis. Si entre los archivos existen resultados en conflicto, usted podría recibir un resultado aprobado y uno con errores.

Asegúrese siempre de verificar los resultados en sus informes.



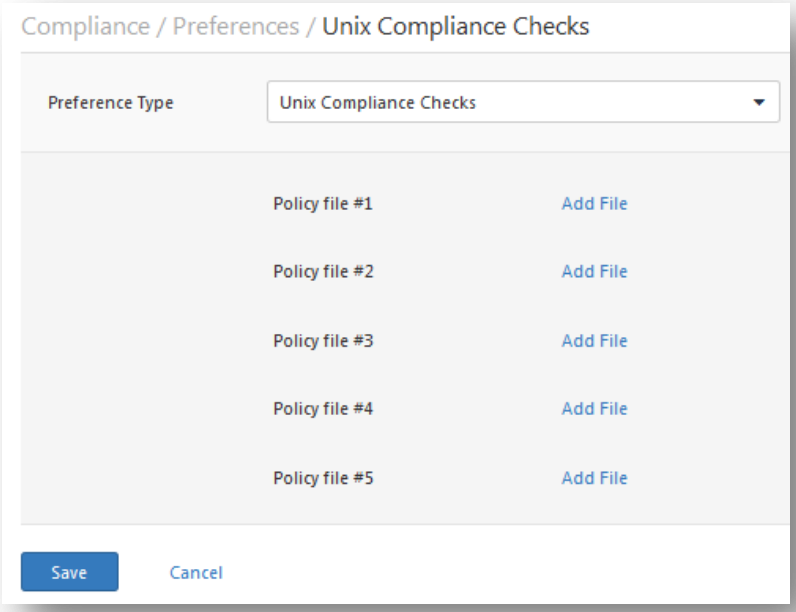
Para crear una directiva de análisis, ingrese en la interfaz de usuario de Nessus, realice una autenticación y seleccione “Policies” (Directivas). Modifique una directiva existente o cree una nueva. Puede especificar las credenciales para acceder al servidor de destino en la ficha “**Credentials**” (Credenciales) de la izquierda.

En la ficha **“Plugins”** (Plugins), habilite la familia de plugins “Policy Compliance” (Compatibilidad con directivas) y asegúrese de que la opción **`"auto_enable_dependencies"`** esté establecida en **“yes”** (sí) en Advanced Settings (Configuración avanzada) (esta es la configuración predeterminada):



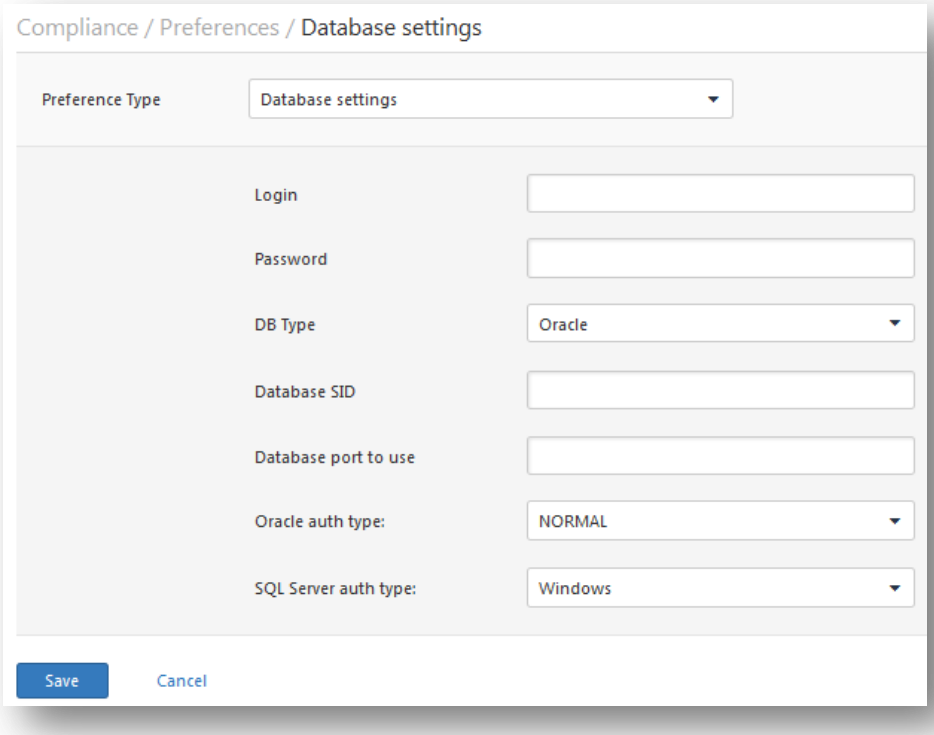
Modificación de una directiva de análisis para determinar si se encuentra disponible Policy Compliance (Compatibilidad con directivas)

Para habilitar el uso de un archivo **`.audit`**, en la ficha "**Preferences**" (Preferencias), seleccione "Cisco IOS Compliance Checks" (Comprobaciones de compatibilidad de Cisco IOS), "Unix Compliance Checks" (Comprobaciones de compatibilidad de Unix), "Windows Compliance Checks" (Comprobaciones de compatibilidad de Windows), "Windows File Content Compliance Checks" (Comprobaciones de compatibilidad de contenido de archivos de Windows), "IBM iSeries Compliance Checks" (Comprobaciones de compatibilidad de IBM iSeries) o "Database Compliance Checks" (Comprobaciones de compatibilidad de bases de datos) en el menú desplegable. En cada sección encontrará cinco campos que pueden especificar archivos **`.audit`** independientes. Los archivos especificados deberán haberse descargado previamente en el sistema del cliente local desde el Tenable Support Portal (Portal de soporte de Tenable).



Ejemplo de cuadro de diálogo de la Interfaz de usuario de Nessus para especificar archivos .audit de Unix

Si se seleccionó “Database Compliance Checks” (Comprobaciones de compatibilidad de bases de datos) en el menú desplegable anterior, los parámetros de inicio de sesión para la base de datos deben introducirse en “**Preferences**” -> “**Database Settings**” (Preferencias -> Configuración de base de datos):



En “Database Settings” (Configuración de base de datos), se encuentra disponible una serie de opciones, que son las siguientes:

Opción	Descripción
Login (Inicio de sesión)	El nombre de usuario para la base de datos.
Password (Contraseña)	La contraseña correspondiente al nombre de usuario proporcionado.
DB Type (Tipo de base de datos)	Se admiten Oracle, SQL Server, MySQL, DB2, Informix/DRDA y PostgreSQL.
Database SID (SID de base de datos)	La identificación de sistema de la base de datos para auditar. Solo se aplica a Oracle, DB2 e Informix.
Oracle auth type (Tipo de autenticación de Oracle)	Se admiten NORMAL, SYSOPER y SYSDBA.
SQL Server auth type (Tipo de autenticación de SQL Server)	Se admiten Windows o SQL Server.

Consulte al administrador de su base de datos local para obtener los valores correctos para estos campos.

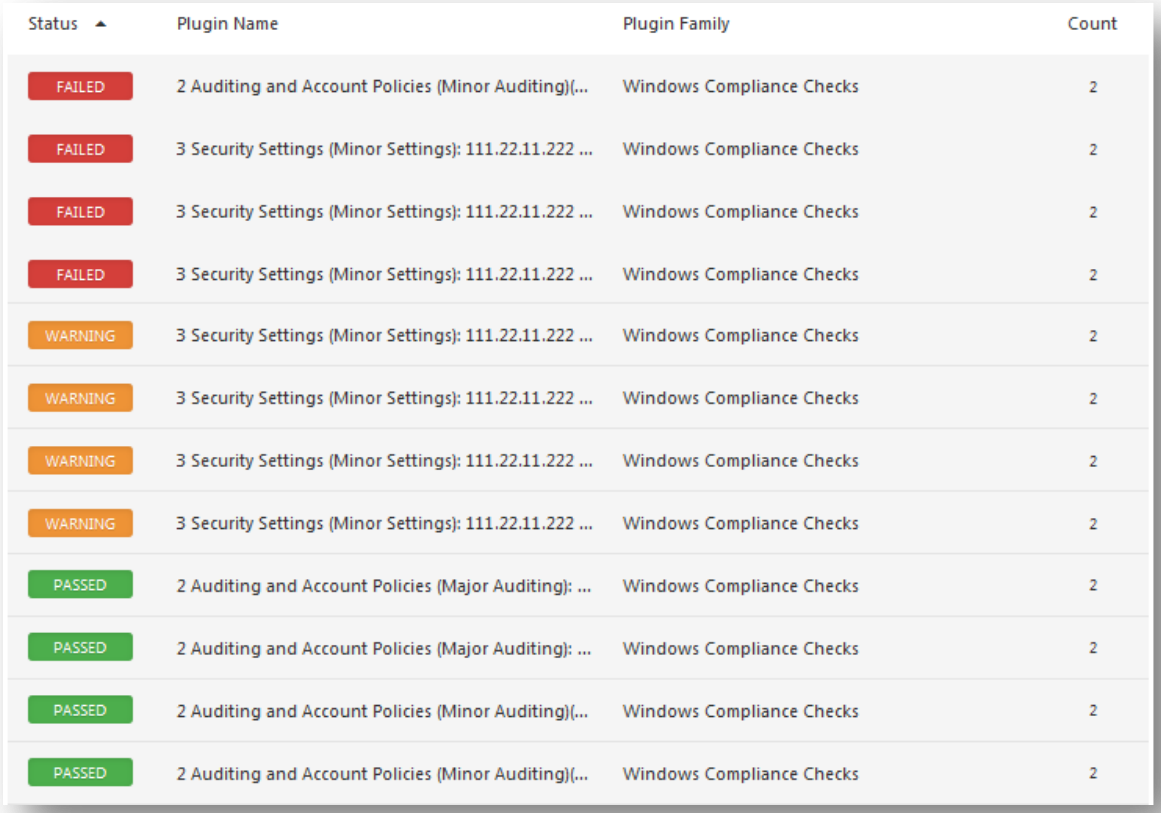
Al llegar a este punto haga clic en “Save” (Guardar), que se encuentra en la parte inferior de la ventana, para finalizar la configuración. La nueva directiva de análisis se añadirá a la lista de directivas de análisis administradas.

Realización de un análisis

Ejecutar un análisis con las comprobaciones de compatibilidad habilitadas es lo mismo que ejecutar otros análisis de auditoría de revisiones locales, o incluso ejecutar análisis de red normales. De hecho, se pueden mezclar y asociar para que se ejecuten al mismo tiempo, si así lo desea.

Ejemplo de resultados

En Nessus se devuelven todos los resultados de compatibilidad con la identificación del plugin que lleva a cabo la prueba. En el ejemplo a continuación, todos los datos devueltos que corresponden a un servidor de Windows analizado corresponderán al plugin `.nbin` de Windows Compliance (Compatibilidad de Windows), que se identificará como plugin 21156.



Status	Plugin Name	Plugin Family	Count
FAILED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2

Ejemplo de resultados de compatibilidad al analizar un servidor de Windows

El informe HTML, que se puede descargar desde la ficha “Reports” (Informes) en la interfaz de usuario de Nessus, destaca las pruebas de compatibilidad aprobadas con azul y las indica mediante el mensaje “PASSED” (APROBADO). Las pruebas no aprobadas se indican con rojo y el mensaje “FAILED” (NO APROBADO). Los elementos que no se pudieron auditar se destacan en amarillo y se indican con el mensaje “WARNING” (ADVERTENCIA).

En el ejemplo anterior solo se muestran cuatro elementos. Cada uno de ellos corresponde a una directiva de control de acceso que comprueba la existencia de protocolos y servicios poco seguros e innecesarios. Algunos de estos servicios no se encontraban en ejecución y cumplían con las expectativas de la directiva `.audit`, mientras que otros (tales como el servicio de “remote registry" [registro remoto]) se encontraban en ejecución y se indicaron como “FAILED” (NO APROBADO). Se recomienda enfáticamente que los elementos que aparecen como “FAILED” (NO APROBADO) se configuren para cumplir con la directiva, de acuerdo con sus normas de seguridad.

Ejemplo de uso de líneas de comandos de Nessus para Unix

Obtención de las comprobaciones de compatibilidad

Si su instalación comercial de Nessus se configuró, habrá cinco archivos de compatibilidad `.nbin` en su directorio de plugins.

Descargue los archivos `.audit` que necesite desde el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/, y colóquelos en el directorio de plugins de su analizador. En la mayoría de las distribuciones, la ubicación predeterminada es el siguiente directorio:

```
/opt/nessus/lib/nessus/plugins
```

Estos plugins se encontrarán presentes junto con más de 40 000 archivos plugin **.nasl** usados por Nessus para realizar análisis de vulnerabilidades. Puede buscarlos a través de la extensión **.nbin**, como se muestra a continuación:

```
# ls compliance*nbin database*nbin unix*nbin cisco_compliance*nbin

cisco_compliance_check.nbin                    database_compliance_check.nbin
compliance_check.nbin                          unix_compliance_check.nbin
compliance_check_windows_file_content.nbin
```

Es posible que haya otros archivos **.nbin** proporcionados por Tenable, tales como el plugin de Skype, que no estén relacionados en absoluto con la realización de comprobaciones de compatibilidad.

Si no tiene acceso local al demonio de Nessus real pero sí cuenta con un nombre de usuario y contraseña para iniciar sesión en el servidor, puede solicitar una lista de plugins mediante la opción "**-p**" del cliente de líneas de comandos **nessus**, como se muestra a continuación:

```
# /opt/nessus/bin/nessus -xp 192.168.20.1 1241 username password | grep 21156
*** The plugins that have the ability to crash remote services or hosts You should
      activate them if you want your security audit to be complete
21156|Policy Compliance|Checks if the remote system is compliant with the
      policy|infos|This script is Copyright (C) 2006 Tenable Network Security|Check
      compliance policy|$Revision: 1.3 $|NOCVE|NOBID|NOXREF|\nSynopsis :\n\n
      Compliance checks\n\nDescription :\n\nUsing the supplied credentials this
      script perform a compliance\ncheck against the given policy.\n\nRisk factor
      :\n\nNone
```

La consulta puede tardar unos minutos para ejecutarse. Si su consulta se ejecuta correctamente pero no devuelve ningún dato, significa que las comprobaciones de compatibilidad no están instaladas en el analizador Nessus remoto.

Uso de archivos .nessus

Nessus cuenta con capacidad para guardar directivas de análisis configuradas, destinos de red e informes como archivos **.nessus**. La sección "Example Nessus User Interface Usage" (Ejemplo de uso de interfaz de usuario de Nessus) describe cómo crear un archivo **.nessus** que contenga una directiva de análisis para las comprobaciones de compatibilidad. 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

El cliente de líneas de comandos de Nessus también tiene la capacidad de exportar directivas de análisis configuradas como archivos **.nessusrc**. Esto puede resultar conveniente para ayudar a habilitar el análisis de líneas de comandos. La sección "Example Nessus User Interface Usage" (Ejemplo de uso de interfaz de usuario de Nessus) describe los pasos para crear una directiva de análisis para las comprobaciones de compatibilidad en Nessus.

Para invocar un análisis de líneas de comandos con Nessus, usted necesita especificar lo siguiente:

- Los plugins de comprobación de compatibilidad de Unix, Windows o bases de datos;
- Las credenciales para los hosts de destino que se están analizando;
- Un archivo **.audit**, o más, para que se ejecuten los plugins de comprobaciones de compatibilidad;
- Que las dependencias se han habilitado.

Las entradas relevantes en un archivo **.nessusrc** tienen el siguiente formato (se omitió cierto contenido):

```
begin(SERVER_PREFS)
…
auto_enable_dependencies = yes
…
end(SERVER_PREFS)
begin(PLUGINS_PREFS)
…
Compliance policy file(s) : = federal_nsa_microsoft_xp_file_permissions.audit
…
end(PLUGINS_PREFS)
begin(PLUGIN_SET)
 21156 = yes
 21157 = yes
…
End(PLUGIN_SET)
```

El ejemplo anterior no incluyó muchos otros datos que especifican las acciones que puede realizar un análisis. El contenido omitido incluye la habilitación del archivo de directiva específico **.audit** que se está usando, la habilitación de las dependencias y los plugins reales de compatibilidad en sí.

Realización de un análisis

Ejecutar un análisis con las comprobaciones de compatibilidad habilitadas es lo mismo que ejecutar otros análisis de auditoría de revisiones locales, o incluso ejecutar análisis de red normales. De hecho, se pueden mezclar y asociar para que se ejecuten al mismo tiempo, si así lo desea.

Ejemplo de resultados

Al igual que con los clientes GUI, todos los resultados compatibles o no compatibles que se hayan detectado se notifican en el siguiente formato:

```
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Reset lockout account counter
      after" : [FAILED]\n\nRemote value: 30\nPolicy value: 20\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password length" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 8\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password age" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 1\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Maximum password age" :
      [FAILED]\n\nRemote value: 42\nPolicy value: 182\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Enforce password history" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 5\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout threshold" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 3\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout duration" :
      [FAILED]\n\nRemote value: 30\nPolicy value: 60\n\n\n
```

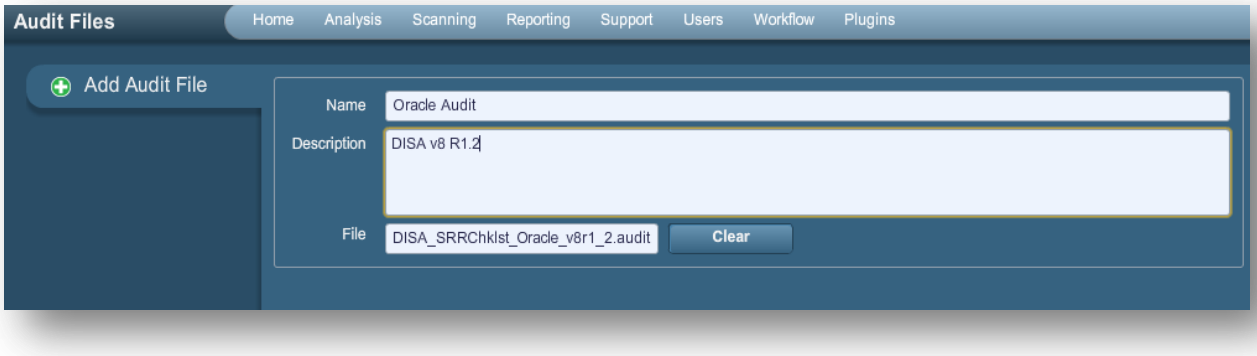
Estos datos se encuentran en el formato de informe **.nsr** para Nessus. Todos ellos son eventos no compatibles.

Uso de SecurityCenter

La información que se indica a continuación tiene como base la ejecución de análisis de compatibilidad con SecurityCenter 4 o una versión más reciente. Si es usuario de Security Center 3.x, consulte “Security Center 3.4 Documentation” (Documentación de Security Center 3.4), disponible en el Tenable Support Portal (Portal de soporte de Tenable): https://support.tenable.com/.

Obtención de las comprobaciones de compatibilidad

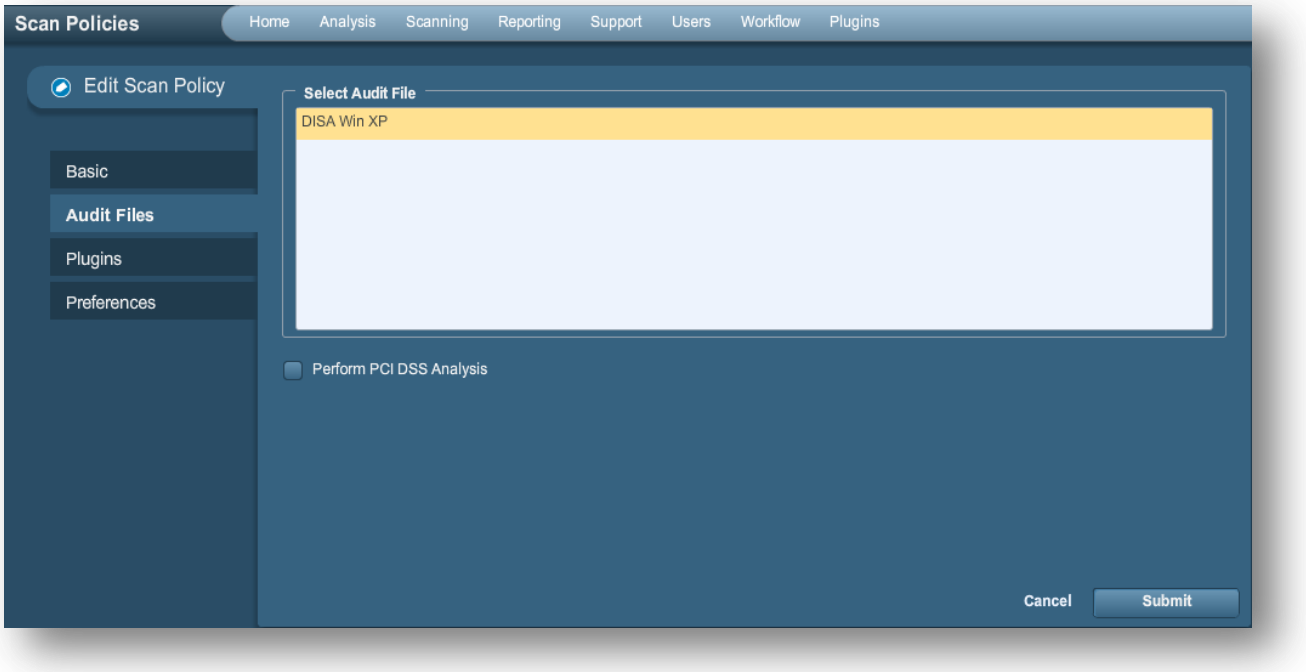
Todos los clientes de SecurityCenter tienen acceso a los plugins comerciales de Nessus. Esto incluye los plugins de comprobación de compatibilidad para Cisco, IBM iSeries, Unix, Windows, Contenido de archivos de Windows y Bases de datos. Estos plugins permiten al usuario cargar y ejecutar análisis de compatibilidad mediante archivos **`.audit`** predefinidos y personalizables, que proporciona Tenable. Obtenga cualquiera de los archivos **`.audit`** requeridos en el Tenable Support Portal (Portal de soporte de Tenable), situado en https://support.tenable.com/. Estos archivos **`.audit`** pueden ser cargados en SecurityCenter por cualquier usuario con el permiso “Create Audit Files” (Crear archivos de auditoría) mediante el uso de la herramienta “Add Audit File” (Agregar archivo de auditoría), que se encuentra en la ficha “Support” (Soporte).



Los archivos **`.audit`** cargados en SecurityCenter estarán disponibles para cualquier usuario de SecurityCenter con el permiso “Create Policies” (Crear directivas). SecurityCenter también se encargará de la distribución de archivos **`.audit`** nuevos y actualizados a los analizadores Nessus.

Configuración de una directiva de análisis para realizar una auditoría de compatibilidad

Para realizar un análisis de compatibilidad con SecurityCenter, los usuarios deben configurar una directiva de análisis con la correspondiente configuración de compatibilidad. Esta directiva especifica las opciones de análisis, los archivos de auditoría, los plugins habilitados y las preferencias avanzadas. La segunda página de “Scan Policy” (Directiva de análisis) especifica los archivos **`.audit`** que se usarán para la auditoría de compatibilidad.



Aquí se pueden seleccionar uno o más archivos **`.audit`** resaltando el archivo **`.audit`** y haciendo clic en "Submit" (Enviar). Para seleccionar varios archivos **`.audit`**, use la tecla "Ctrl" para llevar a cabo una selección múltiple. Si es necesario un análisis PCI DSS básico, antes de enviar la información asegúrese de que la casilla de verificación "Perform PCI DSS Analysis" (Realizar análisis PCI DSS) se encuentre seleccionada.

Los Payment Card Industry Data Security Standards (PCI DSS) (Estándares de seguridad de datos de la industria de tarjetas de pago [PCI DSS]) son un conjunto integral de normas de seguridad establecido por los miembros fundadores del PCI Security Standards Council (Consejo para las normas de seguridad de la industria de las tarjetas de pago), entre los que se incluyen Visa, American Express, Discover Financial Services y MasterCard. PCI DSS tiene como fin proporcionar una base común para salvaguardar los datos confidenciales de los titulares de tarjetas de crédito de todas las marcas de tarjetas bancarias, y es usado por muchos proveedores de comercio electrónico que aceptan y almacenan datos de tarjetas de crédito.

Tenable proporciona a todos los usuarios de SecurityCenter doce plugins que automatizan el proceso de auditorías de PCI DSS. Vea la lista de plugins en la tabla a continuación.

Estos plugins evalúan los resultados y la configuración efectiva de su análisis para determinar si el servidor de destino cumple con los requisitos de compatibilidad de PCI publicados. Los plugins no realizan el análisis en sí. En cambio, recurren a los resultados de otros plugins. Para activar los plugins de PCI DSS, simplemente marque la casilla denominada "Perform PCI DSS Analysis" (Realizar análisis PCI DSS) en la pantalla "Compliance" (Compatibilidad).

Después de seleccionar los archivos **`.audit`** y la configuración PCI DSS deseada, haga clic en la ficha "Plugins" (Plugins) para confirmar la configuración del plugin. Los elementos que se encuentren dentro de la familia de plugins "Policy Compliance" (Compatibilidad con directivas) deben habilitarse en la directiva para llevar a cabo un análisis de compatibilidad.

Cuando el usuario selecciona uno o más archivos de auditoría en la ficha "Audit Files" (Archivos de auditoría) de la directiva de análisis, el plugin correcto se habilita de manera automática en la ficha "Plugins" (Plugins). SecurityCenter analiza los archivos **`.audit`** seleccionados y, de acuerdo con el tipo especificado dentro del archivo, se habilitan los plugins correctos.

En la familia “Policy Compliance” (Compatibilidad con directivas) se encuentran trece plugins disponibles para realizar auditorías de compatibilidad. Estos son los siguientes:

Identificación del plugin	Nombre del plugin	Descripción del plugin
21156	Windows Compliance Checks (Comprobaciones de compatibilidad de Windows)	Usado para auditar opciones de configuración habituales de Windows.
21157	Unix Compliance Checks (Comprobaciones de compatibilidad de Unix)	Usado para auditar opciones de configuración habituales de Unix.
24760	Windows File Contents Compliance Checks (Comprobaciones de compatibilidad de contenido de archivos de Windows)	Usado para auditar contenidos confidenciales en los archivos de servidores de Windows.
33814	Database Compliance Checks (Comprobaciones de compatibilidad de bases de datos)	Usado para auditar opciones de configuración habituales de bases de datos.
33929	PCI DSS compliance (Compatibilidad PCI DSS)	Determina si el servidor web remoto es vulnerable a ataques de secuencias de comandos de sitios (XSS), implementa criptografía SSL2.0 vieja, ejecuta software obsoleto o se ve afectado por vulnerabilidades peligrosas (puntuación total CVSS >= 4).
57581	PCI DSS Compliance: Database Reachable from the Internet (Compatibilidad PCI DSS: la base de datos se puede acceder desde Internet)	Detecta la presencia de una base de datos a la que se puede acceder desde Internet, lo que da como resultado una auditoría de compatibilidad con errores.
60020	PCI DSS Compliance: Handling False Positives (Compatibilidad PCI DSS: manejo de falsos positivos)	Registra el manejo adecuado de los falsos positivos en análisis PCI DSS.
56208	PCI DSS Compliance: Insecure Communication Has Been Detected (Compatibilidad PCI DSS: se ha detectado una comunicación insegura)	Determina si se ha detectado un puerto, protocolo o servicio inseguro, que daría como resultado no lograr la compatibilidad.
56209	PCI DSS Compliance: Remote Access Software Has Been Detected (Compatibilidad PCI DSS: se ha detectado software de acceso remoto)	Detecta la presencia de software de acceso remoto que daría como resultado no lograr la compatibilidad.
33930	PCI DSS Compliance: Passed (Compatibilidad PCI DSS: aprobado)	Al usar la información de análisis disponible, Nessus no encontró ningún error que deshabilite a este host.
33931	PCI DSS Compliance: Tests Requirements (Compatibilidad PCI DSS: requisitos de prueba)	Analiza si el análisis de Nessus cumple con los requisitos de pruebas de PCI o no. Aun si se aprobaron las pruebas técnicas, es posible que este informe no sea suficiente para certificar el servidor.

46689	Cisco IOS Compliance Checks (Comprobaciones de compatibilidad de Cisco IOS)	Usado para auditar opciones de configuración habituales de dispositivos Cisco.
57860	IBM iSeries Compliance Checks (Comprobaciones de compatibilidad de IBM iSeries)	Usado para auditar opciones de configuración habituales de IBM iSeries.

Administración de credenciales

Una ventaja que aporta SecurityCenter al realizar análisis basados en credenciales es que puede ayudar a administrar las credenciales que se están usando. Las credenciales se crean en SecurityCenter seleccionando la ficha “Support” (Soporte), y haciendo clic en “Credentials” (Credenciales) y luego en “Add” (Agregar).

Las credenciales de Unix, Windows y Cisco se almacenan y administran de forma independiente de la directiva de análisis. Las credenciales se pueden crear con visibilidad “User” (Usuario) para el usuario actual, o bien con visibilidad “Organizational” (Organizacional), en cuyo caso podrán ser usadas por otros usuarios de SecurityCenter. Esto permite a los usuarios trabajar con los resultados de los análisis y realizar nuevos análisis sin tener que saber efectivamente cuáles son las credenciales que requiere el análisis.

Para analizar sistemas de bases de datos es necesario tener credenciales adicionales. Estas credenciales se almacenan en la directiva de análisis y se configuran a través de “Database settings” (Configuración de base de datos) (plugin 33815) en las preferencias de la directiva de análisis. Estas credenciales se configuran de forma independiente de las credenciales especificadas en el párrafo anterior.

Análisis de los resultados

SecurityCenter se puede usar para analizar y presentar informes sobre los datos de compatibilidad devueltos por los análisis de Nessus, de muchas formas. Entre los informes habituales se incluyen:

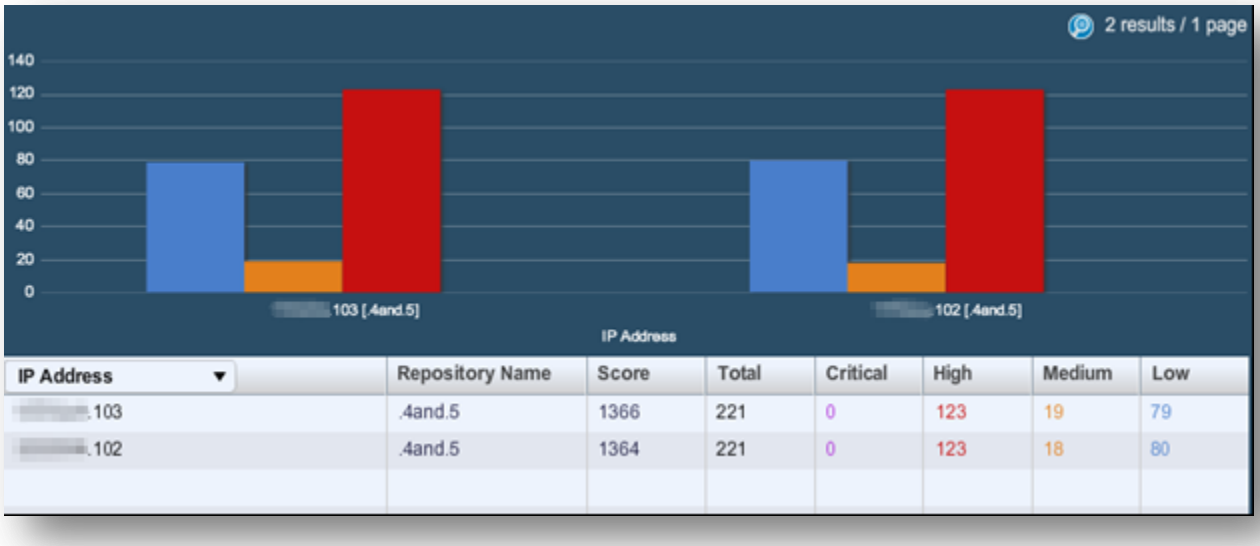
- Enumeración de todas las vulnerabilidades compatibles y no compatibles por grupo de activos
- Enumeración de todas las vulnerabilidades compatibles y no compatibles por host o red
- Resumen de todos los problemas de incompatibilidad
- Auditoría de configuración de bases de datos en busca de errores de configuración habituales
- Informes del estado de los usuarios o del software en función de las necesidades de TI

Una vez que SecurityCenter descubre los datos de compatibilidad, se pueden usar las herramientas analíticas, de tratamiento de incidencias y de informes a fin de determinar el curso de acción más adecuado para volver a configurar los dispositivos auditados. Estos datos se pueden analizar en forma paralela con otras informaciones sobre vulnerabilidades o revisiones de seguridad, o información descubierta de manera pasiva.

A continuación se incluyen algunos ejemplos de capturas de pantalla de SecurityCenter cuando este se usa para analizar información de compatibilidad sobre hosts analizados:

Plugin ID	Total ▼	Severity	Name
1000282	4	Low	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\allocatedasd
1000295	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlog\\AutoAdminLogon
1000294	4	Low	HKLM\\System\\CurrentControlSet\\Control\\SecurePipeServers\\Winreg\\AllowedPaths\\Machine
1000293	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionPipes
1000292	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionShares
1000291	4	Medium	HKLM\\Software\\Policies\\Microsoft\\Cryptography\\ForceKeyProtection
1000290	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\ForceGuest
1000289	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\LimitBlankPasswordUse
1000288	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinClientSec
1000287	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinServerSec
1000286	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\NoDefaultAdminOwner
1000285	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LDAP\\LDAPClientIntegrity
1000284	4	Low	HKLM\\Software\\Microsoft\\Driver Signing\\Policy
1000283	4	High	HKLM\\software\\microsoft\\non-driver signing\\policy
1000296	4	Low	HKLM\\System\\CurrentControlSet\\Control\\FileSystem\\NtfsDisable8dot3NameCreation
1000281	4	High	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\scremoveoption
1000280	4	High	HKLM\\system\\currentcontrolset\\control\\lsa\\lmcompatibilitylevel
1000279	4	High	HKLM\\system\\currentcontrolset\\control\\print\\providers\\lanman print services\\servers\\addprinterdrive
1000278	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\AutoAdminLogon
1000277	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkNoDialIn
1000276	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkHideSharePwds
1000275	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDriveTypeAutoRun
1000274	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\PerformRouterDiscovery
1000273	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\SynAttackProtect
1000272	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\DisableIPSourceRouting
1000271	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\KeepAliveTime
1000270	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableDeadGWDetect
1000269	4	High	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableICMPRedirect

Ejemplo de enumeración de datos de auditorías de compatibilidad con SecurityCenter



IP Address	Repository Name	Score	Total	Critical	High	Medium	Low
.103	.4and.5	1366	221	0	123	19	79
.102	.4and.5	1364	221	0	123	18	80

Ejemplo de enumeración de datos de auditorías de compatibilidad por servidor con SecurityCenter

Para obtener más información sobre el uso de SecurityCenter, consulte la documentación de SecurityCenter que se encuentra disponible en https://support.tenable.com/.

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 5.2): instrucciones sobre cómo configurar y operar la interfaz de usuario de Nessus.
- **Nessus Credential Checks for Unix and Windows** (Comprobaciones con credenciales de Nessus para Unix y Windows): información sobre cómo llevar a cabo análisis de red autenticados mediante el analizador de vulnerabilidades Nessus.
- **Nessus Compliance Checks 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 Active Directory de Microsoft 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://blog.tenable.com/
- 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