IBM Security QRadar Vulnerability Manager
Versión 7.2.6

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que sirve de complemento, lea la información contenida en la sección "Avisos" en la página 103.

Información sobre el producto

Este documento es aplicable a IBM QRadar Security Intelligence Platform V7.2.6 y a los releases subsiguientes a menos que sean reemplazados por una versión actualizada de este documento.

Contenido

Visión general de IBM Security QRadar Vulnerability Manager

Esta información está pensada para ser utilizada con IBM® Security QRadar Vulnerability Manager. QRadar Vulnerability Manager es una plataforma de exploración que se utiliza para identificar, gestionar y priorizar las vulnerabilidades de los activos de la red.

Esta guía contiene instrucciones para configurar y utilizar QRadar Vulnerability Manager en una consola de IBM Security QRadar SIEM o IBM Security QRadar Log Manager.

Público al que va dirigido este manual

Los administradores del sistema encargados de configurar IBM Security QRadar Vulnerability Manager debe tener acceso administrativo a IBM Security QRadar SIEM y a los dispositivos y cortafuegos de la red. El administrador del sistema debe tener conocimientos sobre la red corporativa y sobre tecnologías de red.

Documentación técnica

Para obtener información sobre cómo acceder a más documentación técnica, notas técnicas y notas de release, consulte Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).q

Contactar con el servicio de soporte al cliente

Para obtener información sobre cómo ponerse en contacto con el servicio de soporte al cliente, consulte la página web Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de tecnologías de la información supone proteger los sistemas y la información mediante la prevención, detección y respuesta al acceso no autorizado desde dentro y fuera de la empresa. El acceso no autorizado puede dar como resultado la alteración, destrucción, apropiación indebida o mal uso de la información, y también daños en los sistemas o mal uso de ellos, incluida su utilización para atacar a otros sistemas. Ningún producto o sistema de tecnologías de la información se debe considerar completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir la utilización o acceso no autorizado. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un sistema de seguridad completo, que necesariamente incluye procedimientos operativos adicionales y puede necesitar otros sistemas, productos o servicios para lograr la máxima efectividad. IBM NO GARANTIZA QUE UN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O HAGA QUE SU EMPRESA SEA INMUNE, FRENTE A LA CONDUCTA MALICIOSA O ILEGAL DE UN TERCERO CUALQUIERA.

Capítulo 1. Novedades para los usuarios de QRadar Vulnerability Manager V7.2.6

IBM Security QRadar Vulnerability Manager V7.2.6 presenta mejoras para ayudar a controlar los perfiles de seguridad en el nivel de dominio y a identificar vulnerabilidades de alta prioridad.

Mejorar el enfoque de seguridad integrando IBM BigFix con QRadar Vulnerability Manager

Utilice QRadar Vulnerability Manager con BigFix para identificar vulnerabilidades de alta prioridad y determinar cuáles deben solucionarse en primer lugar. Los fixlets son paquetes predefinidos que pueden desplegarse para corregir vulnerabilidades específicas. QRadar Vulnerability Manager puede publicar automáticamente datos de vulnerabilidad de alta prioridad en el panel de control de BigFix. Los usuarios pueden supervisar y corregir fácilmente las vulnerabilidades de BigFix priorizadas por QRadar Vulnerability Manager.  Más información...

Soporte para entornos multidominio

Utilice los permisos de perfil de seguridad en el nivel de dominio para asegurarse de que se aplica el nivel de acceso correcto para las exploraciones de vulnerabilidades. Ahora puede asociar un explorador con un dominio, utilizar un dominio para la exploración dinámica, asociar un dominio con un perfil de exploración y un resultado de exploración, ver los activos de un dominio que están asociados con una exploración, filtrar informes de exploración por dominio y ver sólo los resultados de exploración y vulnerabilidades que se encuentran en los dominios asociados con el perfil de seguridad.

Capítulo 2. Instalaciones y despliegues de QRadar Vulnerability Manager

Puede acceder a IBM Security QRadar Vulnerability Manager mediante la pestaña **Vulnerabilidades**.

Acceso al panel Vulnerabilidades

Dependiendo del producto que instale o de si actualiza QRadar o instala un nuevo sistema, la pestaña **Vulnerabilidades** puede no aparecer.

- Si instala QRadar SIEM, la pestaña **Vulnerabilidades** se habilita de forma predeterminada con una clave de licencia temporal.
- Si instala QRadar Log Manager, la pestaña **Vulnerabilidades** no está habilitada.
- Dependiendo de cómo actualice QRadar, la pestaña **Vulnerabilidades** puede no estar habilitada.

Para utilizar QRadar Vulnerability Manager después de una instalación o actualización, debe cargar y asignar una clave de licencia válida. Para obtener más información, consulte la *Guía de administración* del producto.

Para obtener más información sobre la actualización, consulte el manual *IBM Security QRadar Upgrade Guide*.

Despliegues de proceso y exploración de vulnerabilidades

Cuando instala y obtiene una licencia para QRadar Vulnerability Manager, se despliega automáticamente un procesador de vulnerabilidades en la consola de QRadar. No se despliega automáticamente un procesador si utiliza una clave de activación de software en la consola de QRadar.

El procesador de vulnerabilidades proporciona de forma predeterminada un componente de exploración. Si es necesario, puede desplegar más exploradores, ya sea en dispositivos exploradores de host gestionados de QRadar Vulnerability Manager o en hosts gestionados de QRadar. Por ejemplo, puede desplegar un explorador de vulnerabilidades en un Recopilador de sucesos o en un QRadar QFlow Collector.

Si es necesario, puede trasladar el procesador de vulnerabilidades a un host gestionado diferente del despliegue. Puede trasladar el procesador para ahorrar espacio de disco en la consola de QRadar.

Restricción: Puede tener un solo procesador de vulnerabilidades en el despliegue. Puede trasladar el procesador de vulnerabilidades solamente a un dispositivo procesador de QRadar Vulnerability Manager dedicado.

Importante: Después de cambiar el despliegue del procesador de vulnerabilidades, debe esperar a que el despliegue se configure completamente. En la página Perfiles de exploración, aparece el mensaje siguiente: **QVM se está desplegando.**

Asegúrese de que Java™ Runtime Environment (JRE) versión 1.7 o IBM Runtime Environment de 64 bits para Java V7.0 esté instalado en todos los sistemas de escritorio que utiliza para acceder a la interfaz de usuario del producto QRadar.

Conceptos relacionados:

"Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7
Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

"Opciones para trasladar el procesador de vulnerabilidades en el despliegue de QRadar Vulnerability Manager" en la página 5
Si es necesario, puede trasladar el procesador de vulnerabilidades desde la consola de QRadar a un dispositivo dedicado de host gestionado de QRadar Vulnerability Manager.

Claves de activación del procesador de vulnerabilidades y del dispositivo explorador

Puede explorar y procesar vulnerabilidades utilizando dispositivos de host dedicados gestionados de QRadar Vulnerability Manager.

Cuando instala un dispositivo procesador o explorador de host gestionado, debe proporcionar una clave de activación válida.

Para obtener más información sobre la instalación de un dispositivo de host gestionado, consulte la *Guía de instalación* del producto.

La clave de activación es una serie alfanumérica de 24 dígitos que consta de cuatro partes y que el usuario recibe de IBM. La clave de activación especifica qué módulos de software corresponden a cada tipo de dispositivo:

- El dispositivo procesador de QRadar Vulnerability Manager incluye los componentes de proceso y exploración de vulnerabilidades.
- El dispositivo explorador de QRadar Vulnerability Manager incluye solamente un componente de exploración de vulnerabilidades.

Puede obtener la clave de activación en los lugares siguientes:

- Si ha adquirido una descarga de software o de dispositivo virtual de QRadar Vulnerability Manager, el correo electrónico de confirmación incluye una lista de claves de activación en el documento adjunto *Guía de inicio*. Puede utilizar este documento para ver el número de pieza correspondiente al dispositivo proporcionado.
- Si ha adquirido un dispositivo que se preinstala con software de QRadar Vulnerability Manager, la clave de activación está incluida en la caja de transporte o CD.

Copia de seguridad y recuperación de datos de vulnerabilidad

Puede utilizar las prestaciones de utilizar y recuperación de IBM Security QRadar SIEM para realizar copias de seguridad y restaurar datos de vulnerabilidad y configuración de IBM Security QRadar Vulnerability Manager.

Cuando se instala QRadar Vulnerability Manager, las copias de seguridad nocturnas o bajo demanda de QRadar SIEM incluyen perfiles de exploración, resultados de exploración e información de configuración de QRadar Vulnerability Manager.

Puede configurar datos o copias de seguridad de configuración mediante el separador **Admin**.

Para obtener más información sobre la copia de seguridad y la recuperación, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Opciones para trasladar el procesador de vulnerabilidades en el despliegue de QRadar Vulnerability Manager

Si es necesario, puede trasladar el procesador de vulnerabilidades desde la consola de QRadar a un dispositivo dedicado de host gestionado de QRadar Vulnerability Manager.

Por ejemplo, puede trasladar el proceso de vulnerabilidades a un host gestionado para ahorrar espacio de disco en la consola de QRadar.

Restricción: Puede tener un solo procesador de vulnerabilidades en el despliegue. Además, debe desplegar el procesador de vulnerabilidades solamente en una consola de QRadar o en un dispositivo procesador de host gestionado de QRadar Vulnerability Manager.

Para trasladar el procesador de vulnerabilidades, elija una de las opciones siguientes:

Opción 1: despliegue un dispositivo procesador dedicado de QRadar Vulnerability Manager

Para desplegar un dispositivo procesador, realice las tareas siguientes:

1. Instale un dispositivo procesador de QRadar Vulnerability Manager dedicado.
2. Añada el dispositivo procesador de host gestionado a QRadar Console mediante la herramienta **Gestión del sistema y licencias** en la pestaña Admin.

   Cuando selecciona la opción de host gestionado, el procesador se elimina automáticamente de la consola de QRadar.

Opción 2: traslade el procesador de vulnerabilidades desde la consola al host gestionado

Si el procesador de vulnerabilidades está en la consola de QRadar, posteriormente puede trasladar el procesador de vulnerabilidades a un dispositivo procesador de host gestionado de QRadar Vulnerability Manager que ha instalado previamente.

En cualquier momento, puede trasladar el procesador de vulnerabilidades de nuevo a la consola de QRadar.

Desplegar un dispositivo procesador dedicado de QRadar Vulnerability Manager

Puede desplegar un dispositivo procesador de QRadar Vulnerability Manager dedicado como host gestionado.

Cuando despliega el procesador de vulnerabilidades en un host gestionado, todas las vulnerabilidades se procesan en el host gestionado.

Restricción: Después de desplegar el procesador de vulnerabilidades en un host gestionado dedicado de QRadar Vulnerability Manager, los perfiles de exploración o resultados de exploración que están asociados a un procesador de consola de QRadar no se muestran. Puede continuar para buscar y ver datos de vulnerabilidad en las páginas **Gestionar vulnerabilidades**.

Antes de empezar

Compruebe que esté instalado un host gestionado dedicado de QRadar Vulnerability Manager y que se haya aplicado una clave de activación válida de dispositivo procesador. Para obtener más información, consulte la *Guía de instalación* del producto.

Procedimiento

1. Inicie una sesión en QRadar Console como administrador:

   `https://`*`Dirección_IP_QRadar`*

   El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root que se especificó durante la instalación.
2. Pulse la pestaña **Admin**.
3. En el panel **Configuración del sistema**, pulse **Gestión del sistema y licencias**.
4. En la tabla de hosts, pulse el host de QRadar Console, pulse > **Acciones de despliegue** > **Añadir host**.
5. Escriba la dirección IP del host y la contraseña.
6. Pulse **Añadir**.
7. Cierre la ventana Gestión del sistema y licencias.
8. En la barra de herramientas del panel **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
9. Pulse **Aceptar**.

Conceptos relacionados:

"Claves de activación del procesador de vulnerabilidades y del dispositivo explorador" en la página 4
Puede explorar y procesar vulnerabilidades utilizando dispositivos de host dedicados gestionados de QRadar Vulnerability Manager.

Tareas relacionadas:

"Verificar que se ha desplegado un procesador de vulnerabilidades" en la página 7
En IBM Security QRadar Vulnerability Manager, puede verificar que el procesador de vulnerabilidades se ha desplegado en una consola de QRadar o host gestionado de QRadar Vulnerability Manager.

Trasladar el procesador de vulnerabilidades a un host gestionado o consola

Si es necesario, puede trasladar el procesador de vulnerabilidades entre un dispositivo de host gestionado de QRadar Vulnerability Manager y la consola de QRadar.

Antes de empezar

Compruebe que esté instalado un host gestionado dedicado de QRadar Vulnerability Manager y que se haya aplicado una clave de activación válida de dispositivo procesador.

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
2. Pulse **Habilitar procesador**.
3. Seleccione una consola o un host gestionado en la lista **Procesador**.

Si el procesador reside en el host gestionado, puede seleccionar solamente la consola de QRadar.

4. Pulse **Guardar**.
5. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
6. Pulse **Aceptar**.

Conceptos relacionados:

"Claves de activación del procesador de vulnerabilidades y del dispositivo explorador" en la página 4
Puede explorar y procesar vulnerabilidades utilizando dispositivos de host dedicados gestionados de QRadar Vulnerability Manager.

Verificar que se ha desplegado un procesador de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede verificar que el procesador de vulnerabilidades se ha desplegado en una consola de QRadar o host gestionado de QRadar Vulnerability Manager.

Procedimiento

1. Inicie una sesión en la consola de QRadar.
2. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
3. Verifique que el procesador aparezca en la lista **Procesador**.

Eliminar un procesador de vulnerabilidades en la consola o host gestionado

Si es necesario, puede eliminar el procesador de vulnerabilidades de una consola de QRadar o de un host gestionado de QRadar Vulnerability Manager.

Procedimiento

1. Inicie una sesión en la consola de QRadar.
2. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestión de despliegue de vulnerabilidades**.
3. Pulse el recuadro de selección **Habilitar procesador** para desmarcarlo.
4. Pulse **Eliminar**.
5. Pulse **Guardar**.
6. Cierre la ventana Gestión del sistema y licencias.
7. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
8. Pulse **Aceptar**.

Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager

Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

El procesador de QRadar Vulnerability Manager se despliega automáticamente con un componente de exploración. Con el despliegue de más exploradores puede

aumentar la flexibilidad de las operaciones de exploración. Por ejemplo, puede explorar áreas determinadas de la red mediante exploradores diferentes en momentos planificados diferentes.

Exploraciones de vulnerabilidades dinámicas

Puede que los exploradores de vulnerabilidades desplegados no tengan acceso a todas las áreas de la red. En QRadar Vulnerability Manager, puede asignar exploradores diferentes a rangos de CIDR de red. Durante una exploración, cada activo comprendido dentro del rango de CIDR que desee explorar se asocia dinámicamente al explorador adecuado.

Para añadir más exploradores de vulnerabilidades, elija cualquiera de las opciones siguientes:

Despliegue un dispositivo explorador dedicado de host gestionado de QRadar Vulnerability Manager

Puede buscar vulnerabilidades mediante un dispositivo explorador dedicado de host gestionado de QRadar Vulnerability Manager.

Para desplegar un dispositivo explorador, realice las tareas siguientes:

1. Instale un dispositivo explorador dedicado de host gestionado de QRadar Vulnerability Manager.
2. Añada el dispositivo explorador de host gestionado a QRadar Console mediante la herramienta **Gestión del sistema y licencias** en la pestaña **Admin**.

Despliegue un explorador de QRadar Vulnerability Manager en la consola o host gestionado de QRadar.

Si traslada el procesador de vulnerabilidades desde la consola de QRadar a un host gestionado de QRadar Vulnerability Manager, puede añadir un explorador a la consola.

También puede añadir un explorador de vulnerabilidades a cualquier host gestionado de QRadar que ya exista en el despliegue. Por ejemplo, puede añadir un explorador a un recopilador de sucesos, recopilador de flujos o procesador de sucesos.

Configure el acceso a un explorador alojado en IBM y explore la zona desmilitarizada (DMZ) de la red

Puede configurar el acceso a un explorador alojado en IBM y explorar los activos situados en la zona desmilitarizada (DMZ).

Conceptos relacionados:

"Exploraciones de vulnerabilidades dinámicas" en la página 58
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración para utilizar determinados exploradores de vulnerabilidades con rangos de CIDR determinados de la red. Por ejemplo, los exploradores pueden tener acceso solamente a determinadas áreas de la red.

Tareas relacionadas:

"Asociar exploraciones de vulnerabilidades a rangos de CIDR" en la página 59
En IBM Security QRadar Vulnerability Manager, para realizar una exploración dinámica, debe asociar exploradores de vulnerabilidades a segmentos diferentes de la red.

"Explorar rangos de CIDR con exploradores de vulnerabilidades diferentes" en la página 60
En IBM Security QRadar Vulnerability Manager, puede explorar áreas de una red con diferentes exploradores de vulnerabilidades.

Desplegar un dispositivo explorador dedicado de QRadar Vulnerability Manager

Puede desplegar un dispositivo explorador dedicado de host gestionado de QRadar Vulnerability Manager.

Antes de empezar

Compruebe que esté instalado un dispositivo explorador dedicado de host gestionado de QRadar Vulnerability Manager y que se haya aplicado una clave de activación válida de dispositivo.

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Añadir host gestionado**.
2. Escriba la dirección IP del host y la contraseña del dispositivo explorador de host gestionado de QRadar Vulnerability Manager.
3. Pulse **Añadir**.

   Debe esperar varios minutos mientras se añade el host gestionado.
4. Cierre la ventana Gestión del sistema y licencias.
5. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
6. Pulse **Aceptar**.

Conceptos relacionados:

"Claves de activación del procesador de vulnerabilidades y del dispositivo explorador" en la página 4
Puede explorar y procesar vulnerabilidades utilizando dispositivos de host dedicados gestionados de QRadar Vulnerability Manager.

Desplegar un explorador de vulnerabilidades en una consola o host gestionado de QRadar

Puede desplegar un explorador de QRadar Vulnerability Manager en una consola de QRadar o host gestionado de QRadar. Por ejemplo, puede desplegar un explorador en un recopilador de flujos, procesador de flujos, recopilador de sucesos o procesador de sucesos.

Antes de empezar

Para desplegar un explorador en la consola de QRadar, el procesador de vulnerabilidades se debe haber trasladado a un dispositivo de host gestionado dedicado de QRadar Vulnerability Manager.

Para desplegar exploradores en hosts gestionados de QRadar, deben existir hosts gestionados en el despliegue. Para obtener más información, consulte la *Guía de instalación* del producto.

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
2. Pulse **Añadir exploradores de vulnerabilidad adicionales**.
3. Pulse el icono **+**.
4. En la lista **Host**, seleccione la consola o el host gestionado de QRadar.

Restricción: No puede añadir un explorador a una consola de QRadar cuando el procesador de vulnerabilidades reside en la consola. Debe trasladar el procesador de vulnerabilidades a un host gestionado de QRadar Vulnerability Manager.

5. Pulse **Guardar**.
6. Cierre la ventana Gestión del sistema y licencias.
7. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
8. Pulse **Aceptar**.
9. Consulte la lista **Servidor de exploración** de la página Configuración de perfil de exploración para asegurarse de que el explorador se ha añadido.

   Para obtener más información, consulte "Crear un perfil de exploración" en la página 31.

Qué hacer a continuación

Ejecute una actualización automática después de añadir el explorador u otro host gestionado con prestaciones de exploración. También puede explorar después de que se ejecute la actualización automática diaria planificada.

Tareas relacionadas:

"Trasladar el procesador de vulnerabilidades a un host gestionado o consola" en la página 6
Si es necesario, puede trasladar el procesador de vulnerabilidades entre un dispositivo de host gestionado de QRadar Vulnerability Manager y la consola de QRadar.

Explorar activos de la zona desmilitarizada

En IBM Security QRadar Vulnerability Manager, puede conectar con un explorador externo y explorar los activos de la zona desmilitarizada de la red para buscar vulnerabilidades.

Si desea explorar activos de la zona desmilitarizada para buscar vulnerabilidades, no necesita desplegar un explorador en la zona desmilitarizada. Debe configurar QRadar Vulnerability Manager con un explorador alojado en IBM que está situado fuera de la red.

El procesador procesa las vulnerabilidades detectadas en la consola de QRadar o host gestionado de QRadar Vulnerability Manager.

Procedimiento

1. Configure la red y los activos para exploraciones externas.
2. Configure QRadar Vulnerability Manager para explorar activos externos.

Configurar la red y activos para exploraciones externas

Para explorar los activos de la zona desmilitarizada (DMZ) de la red, debe configurar la red y notificar a IBM los activos que desee explorar.

Procedimiento

1. Configure el acceso saliente de Internet en el puerto 443.
2. Envíe la información siguiente a `QRadar-QVM-Hosted-Scanner@hursley.ibm.com`:
   - La dirección IP externa de su empresa.

Restricción: La dirección IP debe estar configurada para poder ejecutar exploraciones externas.

- El rango de direcciones IP de los activos contenidos en la zona desmilitarizada.

Configurar QRadar Vulnerability Manager para explorar activos externos

Para explorar los activos de la zona desmilitarizada, debe configurar QRadar Vulnerability Manager mediante la herramienta **Gestión del sistema y licencias** en la pestaña Admin.

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
2. Pulse **Utilizar explorador externo**.
3. En el campo **IP de pasarela**, escriba una dirección IP externa.

   Restricción: La dirección IP externa debe estar configurada para poder explorar activos externos. Envíe por correo electrónico los detalles de su dirección IP externa a IBM.
4. Opcional: Si la red está configurada para utilizar un servidor proxy, pulse **Habilitar servidor proxy** y escriba los detalles del servidor.
5. Pulse **Guardar** y, a continuación, pulse **Cerrar**.
6. En la barra de herramientas del panel **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
7. Pulse **Aceptar**.

   Nota: Las exploraciones autenticadas no se llevan a cabo desde el explorador externo.

Navegadores web soportados

Para que las funciones de los productos IBM Security QRadar trabajen debidamente, debe utilizar un navegador web soportado.

Cuando accede al sistema de QRadar, se le solicita un nombre de usuario y una contraseña. El administrador debe configurar de antemano el nombre de usuario y la contraseña.

La tabla siguiente lista las versiones soportadas de navegadores web.

Tabla 1. Navegadores web soportados para productos QRadar

Navegador web	Versiones soportadas
Mozilla Firefox	38.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, con la modalidad de documento y la modalidad de navegador habilitadas.	10.0 11.0
Google Chrome	Versión 46

Habilitar la modalidad de documento y la modalidad de navegador en Internet Explorer

Si utiliza Microsoft Internet Explorer para acceder a productos de IBM Security QRadar, debe habilitar la modalidad de navegador y la modalidad de documento.

Procedimiento

1. En el navegador web Internet Explorer, pulse F12 para abrir la ventana Herramientas de desarrollado.
2. Pulse **Modo de explorador** y seleccione la versión que utilice del navegador web.
3. Pulse **Modo de documento** y seleccione el **Estándar Internet Explorer** correspondiente al release de Internet Explorer.

Ampliación del periodo de licencia temporal de QRadar Vulnerability Manager

De forma predeterminada, cuando se instala IBM Security QRadar SIEM, puede ver la pestaña **Vulnerabilidades** porque también se ha instalado una clave de licencia temporal. Cuando caduca la licencia temporal, puede ampliarla cuatro semanas más.

Procedimiento

1. En la pestaña **Admin**, pulse el icono **Gestor de vulnerabilidades** en el área **Inténtelo**.
2. Para aceptar el acuerdo de licencia de usuario final, pulse **Aceptar**.

   Cuando el periodo de licencia ampliado finaliza, debe esperar seis meses para poder activar la licencia temporal de nuevo. Para tener acceso permanente a QRadar Vulnerability Manager, debe adquirir una licencia.

Capítulo 3. IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager es una plataforma de exploración de red que detecta vulnerabilidades dentro de aplicaciones, sistemas y dispositivos de una red o dentro de la zona desmilitarizada (DMZ).

QRadar Vulnerability Manager utiliza inteligencia y seguridad para ayudarle a gestionar y priorizar las vulnerabilidades de la red. Por ejemplo, puede utilizar QRadar Vulnerability Manager para supervisar continuamente vulnerabilidades, mejorar la configuración de recursos e identificar parches de software. Puede también priorizar déficits de seguridad asociando datos de vulnerabilidad con flujos de red, datos de registro, cortafuegos y datos del sistema de prevención de intrusiones (IPS).

Puede mantener una visibilidad en tiempo real de las vulnerabilidades que son detectadas por el explorador incorporado de QRadar Vulnerability Manager y por exploradores externos. Los exploradores externos se integran con QRadar e incluyen IBM BigFix, Guardium, AppScan, Nessus, nCircle y Rapid 7.

A menos que se indique lo contrario, todas las referencias a QRadar Vulnerability Manager hacen referencia a IBM Security QRadar Vulnerability Manager. Todas las referencias a QRadar hacen referencia a IBM Security QRadar SIEM e IBM Security QRadar Log Manager, y todas las referencias a SiteProtector hacen referencia a IBM Security SiteProtector.

Exploración de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, la exploración de vulnerabilidades se controla configurando perfiles de exploración. Cada perfil de exploración especifica los activos que desee explorar y la planificación de exploración.

procesador de vulnerabilidades

Cuando instala y obtiene una licencia para QRadar Vulnerability Manager, se despliega automáticamente un procesador de vulnerabilidades en la consola de QRadar. El procesador contiene un componente de exploración de QRadar Vulnerability Manager.

Opciones de despliegue

La exploración de vulnerabilidades se puede desplegar de maneras diferentes. Por ejemplo, puede desplegar la capacidad de exploración en un dispositivo explorador de host gestionado de QRadar Vulnerability Manager o en un host gestionado de QRadar.

Opciones de configuración

Los administradores pueden configurar exploraciones de las formas siguientes:

- Planificar exploraciones para que se ejecuten en momentos adecuados para los activos de la red.
- Especificar las horas durante las cuales no se deben ejecutar exploraciones.

- Especificar activos que desee excluir de las exploraciones, ya sea globalmente o para cada exploración.
- Configurar exploraciones de parches autenticadas para los sistemas operativos Linux, UNIX o Windows.
- Configurar protocolos de exploración diferentes o especificar los rangos de puertos que desee explorar.

Conceptos relacionados:

"Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7
Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

"Opciones para trasladar el procesador de vulnerabilidades en el despliegue de QRadar Vulnerability Manager" en la página 5
Si es necesario, puede trasladar el procesador de vulnerabilidades desde la consola de QRadar a un dispositivo dedicado de host gestionado de QRadar Vulnerability Manager.

Iniciación a la exploración de vulnerabilidades

La configuración inicial del sistema de IBM Security QRadar Vulnerability Manager para la gestión de las vulnerabilidades y la red requiere una planificación sistemática.

Hay tres áreas clave que deben tenerse en cuenta cuando se utiliza QRadar Vulnerability Manager para la exploración de vulnerabilidades:

- El tipo de exploración que se ejecutará y con qué frecuencia se ejecutará.
- El número de exploradores que se desplegarán y el número de activos que se explorarán en un momento dado.
- Cómo gestionar las vulnerabilidades que se descubran.

Tipos de exploración

IBM Security QRadar Vulnerability Manager proporciona varios tipos de políticas de exploración predeterminados. También puede definir sus propias exploraciones a partir de plantillas.

A continuación se indican las plantillas utilizadas con más frecuencia:

Exploración de descubrimiento
: Descubre los activos de la red. Después explora los puertos para identificar las características de activos clave como sistema operativo, tipo de dispositivo y los servicios proporcionados por el activo. Las vulnerabilidades no se exploran.

Exploración completa
: Descubre los activos de la red que utilizan un rango de puertos de exploración rápida. Realiza una exploración de los puertos configurables por el usuario y una exploración no autenticada de los servicios descubiertos como FTP, web, SSH y base de datos. Si se proporcionan credenciales, se lleva a cabo una exploración autenticada.

Exploración de parches
: Explora la red para descubrir activos y después realiza una exploración rápida de puertos y una exploración de credenciales de los activos.

Exploraciones de descubrimiento

Una exploración de descubrimiento es una exploración sin credenciales ligera. Busca en un espacio de direcciones las direcciones IP activas y, a continuación, explora sus puertos. Realiza búsquedas DNS y NetBIOS para descubrir qué sistema operativo ejecutan los activos, qué servicios abiertos proporcionan y los nombres de red que tienen asignados.

Por lo general, las exploraciones de descubrimiento se ejecutan con frecuencia. A menudo se ejecutan semanalmente para garantizar a los usuarios de SIEM y SOC una buena visibilidad de los activos de red y la información de activos, como los nombres de activo, el sistema operativo y los servicios abiertos.

Exploraciones completas

Una exploración completa ejecuta la suite completa de pruebas de QRadar Vulnerability Manager.

Una exploración completa tiene estas fases:

1. Una exploración de descubrimiento
2. Comprobaciones sin credenciales. Comprueba los servicios que no requieren credenciales, por ejemplo, lectura de banners y respuestas para obtener información de versión, caducidad del certificado SSL, pruebas de cuentas predeterminadas y prueba de respuestas para vulnerabilidades.
3. Comprobaciones con credenciales. QRadar Vulnerability Manager inicia sesión en el activo y recopila el inventario de aplicaciones y la configuración necesaria; también se generan (o se suprimen) vulnerabilidades según convenga. Las exploraciones de credenciales son preferibles a las exploraciones sin credenciales. Las exploraciones sin credenciales proporcionan una útil visión general de la situación de vulnerabilidad de la red. Sin embargo, la exploración con credenciales es esencial para un programa de gestión de vulnerabilidades integral y exhaustivo.

Nota: Las exploraciones completas a veces pueden bloquear algunas cuentas de administración (por ejemplo, SQL Server) cuando QRadar Vulnerability Manager prueba varias credenciales predeterminadas en esas cuentas.

Exploraciones de parches

Utilice las exploraciones de parches para determinar qué parches y qué productos se han instalado o faltan en la red.

Una exploración de parches tiene dos fases principales:

- Una exploración de descubrimiento
- Comprobaciones sin credenciales

Las exploraciones de parches se ejecutan en menos tiempo y tienen un impacto menor en la red y los activos que se exploran porque no se realizan comprobaciones sin credenciales.

Cuándo explorar

A continuación se proporciona un calendario habitual para cada tipo de exploración:

- Exploración de descubrimiento – Ejecutar semanalmente
- Exploración de parches – Ejecutar cada 1-4 semanas
- Exploración completa – Ejecutar cada 2 ó 3 meses

Conceptos relacionados:

"Planificación de exploración" en la página 37
En IBM Security QRadar Vulnerability Manager, puede planificar las fechas y horas en que es conveniente explorar los activos de red para buscar vulnerabilidades conocidas.

Capítulo 5, "Exploración de vulnerabilidades", en la página 31
En IBM Security QRadar Vulnerability Manager, toda la exploración de la red está controlada por los perfiles de exploración creados por el usuario. Puede crear varios perfiles de exploración y configurar cada perfil de forma diferente de acuerdo con los requisitos específicos de la red.

"Políticas de exploración" en la página 60
Una política de exploración proporciona una ubicación central para configurar los requisitos específicos de exploración.

Tareas relacionadas:

"Crear un perfil de exploración" en la página 31
En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para especificar cómo y cuándo se exploran los activos de la red para buscar vulnerabilidades.

Despliegues de exploradores remotos

Puede desplegar un número ilimitado de exploradores remotos en una red.

Cuando diseñe un despliegue de exploradores remotos, debe tener en cuenta los factores siguientes:

- El número de activos que es necesario explorar.
- La conectividad de red entre IBM Security QRadar Vulnerability Manager y los activos que explora.
- El ancho de banda de red que se necesita.
- Si se va a utilizar la exploración dinámica.
- Cuántas tarjetas de interfaz de red (NIC) se utilizarán en un explorador.

Exploradores y activos

En principio, no hay límite alguno en cuanto al número de activos que un explorador puede explorar. Cada explorador tiene un ancho de banda y las solicitudes de exploración se ponen en cola cuando se ha utilizado todo el ancho de banda.

Cuantos más activos solicite a un explorador que explore, más tiempo tardará la exploración en llevarse a cabo. Por ejemplo, el despliegue de exploradores para explorar hasta 4000 ó 5000 activos da como resultado unos tiempos de exploración aceptables (2 ó 3 días como máximo).

Conectividad de explorador y activo

En general, evite explorar a través de cortafuegos y en conexiones WAN con poco ancho de banda.

Las siguientes directrices le serán de utilidad:

- Mantenga baja la carga en el cortafuegos.
- Reduzca el riesgo de interferencias del cortafuegos con la exploración. Por ejemplo, no permita que el cortafuegos bloquee los puertos que se necesitan para completar la exploración.
- Asegúrese de las exploraciones se ejecutan lo más rápidamente posible.
- Asegúrese de que una conectividad WAN baja no afecte negativamente a las exploraciones.

Valores de límite de ancho de banda

Puede configurar el ancho de banda de red por perfil de exploración en IBM Security QRadar Vulnerability Manager.

Cuando se aumenta el ancho de banda de red por perfil de exploración, QRadar Vulnerability Manager explora más herramientas de vulnerabilidades en paralelo y, por lo tanto, las exploraciones se ejecutan más rápidamente. Puede establecer el límite de ancho de banda en la página Configuración de perfil de exploración. Están disponibles las opciones siguientes:

Opción	Valor de límite de ancho de banda
Bajo	100 Kbps
Medio	1000 Kbps (valor predeterminado)
Alto	5000 Kbps
Completo	máximo de la red

Si está explorando a través de enlaces de ancho de banda de red limitados, no aumente el ancho de banda de red a más de 1000 Kbps. Como norma, cuando efectúe una exploración de parches con el valor **Medio**, QRadar Vulnerability Manager hace una exploración de parches de diez activos en paralelo. Con el valor **Alto**, explora 50 activos en paralelo.

Conceptos relacionados:

"Detalles de perfil de exploración" en la página 35
En IBM Security QRadar Vulnerability Manager puede describir una exploración, seleccionar el explorador que desea utilizar y elegir entre varias opciones de política de exploración.

Tareas relacionadas:

"Crear un perfil de exploración" en la página 31
En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para especificar cómo y cuándo se exploran los activos de la red para buscar vulnerabilidades.

Exploración dinámica

En la exploración dinámica, IBM Security QRadar Vulnerability Manager selecciona un explorador según la dirección IP que se explorará.

La exploración dinámica reduce el número de trabajos de exploración que debe configurar. Por ejemplo, si despliega diez exploradores de QRadar Vulnerability Manager y no utiliza la exploración dinámica, debe configurar diez trabajos de exploración individuales. Debe seleccionar un explorador por cada trabajo de exploración. Si utiliza la exploración dinámica, puede configurar un único trabajo de exploración para utilizar los diez exploradores asociando rangos de CIDR con

cada explorador. QRadar Vulnerability Manager selecciona el explorador apropiado para cada dirección IP que se va a explorar.

La exploración dinámica es más útil cuando se despliegan muchos exploradores. Si tiene, por ejemplo, más de cinco exploradores, con la exploración dinámica puede ahorrar tiempo. Como norma, no habilite la exploración dinámica cuando lleve a cabo el conjunto inicial de las exploraciones de prueba. Puede pasar a la exploración dinámica cuando esté satisfecho con los tiempos y los resultados de exploración.

Conceptos relacionados:

"Exploraciones de vulnerabilidades dinámicas" en la página 58
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración para utilizar determinados exploradores de vulnerabilidades con rangos de CIDR determinados de la red. Por ejemplo, los exploradores pueden tener acceso solamente a determinadas áreas de la red.

Tareas relacionadas:

"Crear un perfil de exploración" en la página 31
En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para especificar cómo y cuándo se exploran los activos de la red para buscar vulnerabilidades.

Tarjetas de interfaz de red en exploradores

En IBM Security QRadar Vulnerability Manager, la exploración no depende de las tarjetas de interfaz de red (NIC) que están configuradas en el dispositivo explorador.

Puede configurar muchas NIC, aunque la configuración habitual es de 4 ó 5. QRadar Vulnerability Manager utiliza protocolos TCP/IP estándar para explorar cualquier dispositivo que tenga una dirección IP. Si se definen varias NIC, la exploración sigue la configuración de red estándar en un dispositivo.

Visión general de la gestión de vulnerabilidades

IBM Security QRadar Vulnerability Manager proporciona un proceso para la gestión de vulnerabilidades que se basa en la asignación de propietarios de activos.

Puede configurar propietarios de activos en la página Asignación de vulnerabilidades de la pestaña **Vulnerabilidades** o mediante una API. Después de asignar los activos, las vulnerabilidades descubiertas en los activos se asignan a esos usuarios o grupos con una fecha de vencimiento en función del nivel de riesgo de las vulnerabilidades en cuestión. También puede también configurar las fechas de vencimiento y el nivel de riesgo en la página Asignación de vulnerabilidades. A continuación, puede configurar informes de remediación para que enviarlos a los usuarios de forma periódica. Utilice los informes de remediación para resaltar las acciones siguientes:

- Los parches que debe instalar.
- Los pasos que es necesario seguir para remediar la vulnerabilidad.
- Los activos que tienen vulnerabilidades vencidas.
- Nuevas vulnerabilidades que se han descubierto desde la última exploración.

Los informes de remediación estándares están disponibles en la pestaña **Correo electrónico** de la página Configuración de perfil de exploración. Puede crear informes de cliente adicionales mediante búsquedas de QRadar Vulnerability Manager. Utilice una amplia gama de criterios de búsqueda para asegurarse de

que los informes se centran en las actividades de remediación de vulnerabilidades que necesita para satisfacer sus necesidades empresariales y de conformidad específicas.

Para facilitar la creación de informes de remediación, QRadar Vulnerability Manager puede crear automáticamente los informes Vulnerabilidades de activos y Vulnerabilidad para cada propietario de activo a partir de una única definición de informe.

Cuando los activos se vuelven a explorar, todas las vulnerabilidades remediadas se detectan automáticamente y se marcan como arregladas. Se eliminan de los informes y las vistas, a menos que se configure explícitamente lo contrario. Todas las vulnerabilidades que se hayan arreglado anteriormente y que se vuelvan a detectar se reabren automáticamente.

Conceptos relacionados:

Capítulo 10, "Informes de vulnerabilidades", en la página 93
En IBM Security QRadar Vulnerability Manager, puede crear un informe o editar un informe existente, o utilizar el asistente de informes para crear, planificar o distribuir un informe nuevo.

Tareas relacionadas:

"Asignar un usuario técnico como propietario de grupos de activos" en la página 89
En IBM Security QRadar Vulnerability Manager puede configurar grupos de activos y asignar automáticamente sus vulnerabilidades a usuarios técnicos.

"Configurar tiempos de corrección para las vulnerabilidades en activos asignados" en la página 91
En IBM Security QRadar Vulnerability Manager, puede configurar tiempos de corrección para diferentes tipos de vulnerabilidades.

"Notificar por correo electrónico el inicio y detención de las exploraciones de vulnerabilidades a los propietarios de activos" en la página 69
Notifique la planificación de exploraciones por correo electrónico a los propietarios de activos. También puede enviar informes por correo electrónico a los propietarios de activos.

"Buscar datos de vulnerabilidad" en la página 72
En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

Panel de control de gestión de vulnerabilidades

Puede visualizar información de vulnerabilidades en el panel de control de QRadar.

IBM Security QRadar Vulnerability Manager se distribuye con un panel de control de vulnerabilidades predeterminado para que el usuario pueda ver rápidamente los riesgos a los que está expuesta su empresa.

Puede crear un panel de control nuevo, gestionar los paneles de control existentes y modificar los valores de visualización de cada elemento del panel de control de vulnerabilidades.

Para obtener más información sobre paneles de control, consulte la *Guía del usuario* del producto.

Revisar datos de vulnerabilidad en el panel de control de gestión de vulnerabilidades predeterminado

Puede ver información de gestión de vulnerabilidades predeterminada en el panel de control de QRadar.

El panel de control de gestión de vulnerabilidades predeterminado contiene información sobre riesgos, vulnerabilidades y exploraciones.

Puede configurar su propio panel de control para que contenga diversos elementos, tales como búsquedas guardadas.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la lista **Mostrar panel de control** de la barra de herramientas, seleccione **Gestión de vulnerabilidades**.

Crear un panel de control de gestión de vulnerabilidades personalizado

En QRadar, puede crear un panel de control de gestión de vulnerabilidades que está personalizado de acuerdo con sus necesidades.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.
3. Escriba un nombre y una descripción para el panel de control de vulnerabilidades.
4. Pulse **Aceptar**.
5. Opcional: En la barra de herramientas, seleccione **Añadir elemento** > **Gestión de vulnerabilidades** y elija una de las opciones siguientes:
   - Si desea mostrar búsquedas guardadas predeterminadas en el panel de control, seleccione **Búsquedas de vulnerabilidades**.
   - Si desea mostrar enlaces de sitios web que apuntan a información sobre seguridad y vulnerabilidades, seleccione **Noticias sobre seguridad**, **Avisos de seguridad** o **Vulnerabilidades publicadas más recientemente**.
   - Si desea mostrar información que está a punto de completar o exploraciones en ejecución, seleccione **Exploraciones completadas** o **Exploraciones en curso**.

Tareas relacionadas:

"Guardar criterios de búsqueda de vulnerabilidades" en la página 77
En IBM Security QRadar Vulnerability Manager, puede guardar criterios de búsqueda de vulnerabilidades para su uso en el futuro.

Crear un panel de control para la conformidad de parches

Cree un panel de control para mostrar el parche más efectivo que se debe utilizar para corregir vulnerabilidades encontradas en la red.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.

3. Escriba un nombre y una descripción para el panel de control de vulnerabilidades.
4. Pulse **Aceptar**.
5. En la barra de herramientas, seleccione **Añadir elemento** > **Gestión de vulnerabilidades** > **Búsquedas de vulnerabilidades** y elija la búsqueda guardada predeterminada que se desee mostrar en el panel de control.
6. En la cabecera del nuevo elemento de panel de control, pulse el icono amarillo **Valores**.
7. Seleccione **Parche** en la lista **Agrupar por** y luego seleccione una de las opciones siguientes en la lista **Representar gráficamente por**:
   - Si desea ver cuántos activos necesitan que se les aplique el parche, seleccione **Recuento de activos**.
   - Si desea ver la puntuación de riesgo acumulada para cada parche, seleccione **Puntuación de riesgo**.
   - Si desea ver el número de vulnerabilidades que están cubiertas por un parche, seleccione **Recuento de vulnerabilidades**.
8. Pulse **Guardar**.
9. Para ver detalles de vulnerabilidad en la página **Gestionar vulnerabilidades** > **Por vulnerabilidad** del panel **Vulnerabilidades**, pulse el enlace **Ver en Por vulnerabilidad** en la parte inferior del elemento de panel de control.

Capítulo 4. Integraciones de software de seguridad

IBM Security QRadar Vulnerability Manager se integra con otros productos de seguridad para ayudarle a gestionar y priorizar los riesgos de seguridad. Las integraciones con otro software amplían las prestaciones de QRadar Vulnerability Manager.

Integración de QRadar Risk Manager y QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager se integra con IBM Security QRadar Risk Manager para ayudarle a priorizar riesgos y vulnerabilidades en la red.

QRadar Risk Manager se instala como dispositivo por separado y después se añade a la consola de QRadar SIEM como host gestionado mediante la herramienta **Gestión del sistema y licencias** en la pestaña Admin.

Para obtener más información sobre la instalación de QRadar Risk Manager, consulte el manual *IBM Security QRadar Risk Manager Installation Guide*.

Políticas de riesgos y priorización de vulnerabilidades

Puede integrar QRadar Vulnerability Manager con QRadar Risk Manager mediante la definición y supervisión de políticas de riesgos para activos o vulnerabilidades.

Cuando se produce el cumplimiento o no cumplimiento de las políticas de riesgos definidas en QRadar Risk Manager, se ajustan las puntuaciones de riesgo de vulnerabilidades en QRadar Vulnerability Manager. Los niveles de ajuste dependen de las políticas de riesgos existentes en la empresa.

Cuando las puntuaciones de riesgo de vulnerabilidades se ajustan en QRadar Vulnerability Manager, los administradores pueden realizar las tareas siguientes:

- Obtener una visión inmediata de las vulnerabilidades que no cumplieron una política de riesgos.

  Por ejemplo, puede aparecer información nueva en el panel de control de QRadar o enviarse por correo electrónico.
- Volver a priorizar las vulnerabilidades que requieren atención inmediata.

  Por ejemplo, un administrador puede utilizar la **Puntuación de riesgo** para identificar rápidamente vulnerabilidades de alto riesgo.

Si aplica políticas de riesgos a nivel de activo en QRadar Risk Manager, se ajustarán las puntuaciones de riesgo de todas las vulnerabilidades del activo en cuestión.

Para obtener más información sobre la creación y supervisión de políticas de riesgos, consulte el manual *IBM Security QRadar Risk Manager User Guide*.

Tareas relacionadas:

"Priorizar vulnerabilidades de alto riesgo mediante la aplicación de políticas de riesgo" en la página 81
En IBM Security QRadar Vulnerability Manager, puede alertar a los administradores respecto a las vulnerabilidades de alto riesgo aplicando políticas de riesgo a las vulnerabilidades.

Integración de BigFix

IBM Security QRadar Vulnerability Manager se integra con IBM BigFix para ayudarle a filtrar y priorizar las vulnerabilidades que se pueden corregir.

Prestaciones de BigFix

Anteriormente denominado IBM Security Endpoint Manager, BigFix proporciona visibilidad y control compartidos entre las operaciones de TI y la seguridad. BigFix identifica vulnerabilidades de alta prioridad y determina cuáles necesitan fixlets en primer lugar. Los fixlets son paquetes que pueden desplegarse para corregir vulnerabilidades específicas. Los fixlets corrigen problemas y vulnerabilidades de forma rápida y eficaz. Desde la consola de BigFix, puede desplegar fixlets simultáneamente en un gran número de puntos finales o activos.

Desde una sola consola, BigFix ofrece la posibilidad de gestionar y controlar una red de cientos de miles de puntos finales o activos, a través de un rango de plataformas y dispositivos que se encuentran en una ubicación geográfica.

BigFix se utiliza para el descubrimiento de activos y la gestión de parches, la distribución de software, el inventario de software y la supervisión de la utilización de software, la gestión del ciclo de vida del sistema, el cumplimiento de la seguridad y la obligatoriedad continua.

Integración de QRadar Vulnerability Manager con BigFix

BigFix proporciona un panel de control que se integra con QRadar Vulnerability Manager. Puede utilizar el panel de control para corregir las vulnerabilidades detectadas por QRadar Vulnerability Manager.

Para habilitar esta conexión y visualizar datos de QRadar Vulnerability Manager en la consola de BigFix, debe realizar pasos de configuración en QRadar Vulnerability Manager.

Por separado, también debe realizar algunos pasos de configuración en BigFix para procesar los datos recibidos desde QRadar Vulnerability Manager. Para obtener información acerca de cómo realizar los pasos de configuración en BigFix, consulte la *Guía del usuario de IBM BigFix QRadar*.

Corrección de vulnerabilidades

Dependiendo de si ha instalado e integrado BigFix, QRadar Vulnerability Manager proporciona información diferente para ayudarle a corregir vulnerabilidades.

- Si BigFix no está instalado, QRadar Vulnerability Manager proporciona información sobre vulnerabilidades para las cuales existe un arreglo.

  QRadar Vulnerability Manager mantiene una lista de información sobre arreglos de vulnerabilidades. La información sobre arreglos está asociada al catálogo de vulnerabilidades conocidas.

  Mediante la búsqueda de QRadar Vulnerability Manager, puede identificar vulnerabilidades para las que existe un arreglo.
- Si BigFix está instalado, QRadar Vulnerability Manager también proporciona detalles específicos sobre el proceso de corrección de vulnerabilidades. Por ejemplo, puede existir un arreglo planificado o un activo puede ya estar corregido.

El servidor de BigFix recoge información sobre arreglos de cada uno de los agentes de BigFix. A intervalos regulares predefinidos se envía información sobre el estado de arreglos a QRadar Vulnerability Manager.

Mediante la función de búsqueda de QRadar Vulnerability Manager, puede identificar rápidamente esas vulnerabilidades cuya corrección está planificada o que ya están corregidas.

Componentes de la integración

Una integración típica consta de los componentes siguientes:

- Una consola de IBM Security QRadar.
- Una instalación con licencia de QRadar Vulnerability Manager.
- Una instalación del servidor de BigFix.
- Una instalación del agente de BigFix en cada destino de exploración de la red.

Hay dos maneras de integrar QRadar Vulnerability Manager con BigFix:

- Configurar BigFix para integrarlo con QRadar Vulnerability Manager para que la información de BigFix se envíe a QRadar Vulnerability Manager. Esta configuración requerirá comunicación SSL.
- Configure QRadar Vulnerability Manager para integrarlo con BigFix para que la información se envíe desde QRadar Vulnerability Manager a BigFix.

Tareas relacionadas:

"Identificar el estado de parche de las vulnerabilidades" en la página 83
En IBM Security QRadar Vulnerability Manager, puede identificar el estado de parche de las vulnerabilidades.

Configurar BigFix para enviar información a QRadar Vulnerability Manager

Puede configurar IBM BigFix para integrarlo con IBM Security QRadar Vulnerability Manager. En este escenario, la información se envía desde BigFix a QRadar Vulnerability Manager.

Esta configuración requiere comunicación SSL y pasos de configuración del adaptador de BigFix.

Antes de empezar

Los componentes siguientes deben estar instalados en la red:

- Un servidor de BigFix.
- Un agente de BigFix en cada activo de la red que desee explorar.

Si utiliza cifrado SSL (capa de sockets seguros), debe configurar SSL para la integración de BigFix.

Procedimiento

1. Para configurar la comunicación SSL, siga estos pasos:
   a. Descargue el certificado de clave pública: abra el navegador web y escriba `https://dirección_IP_servidor_BigFix/webreports`.
   b. Pulse **Añadir excepción** y, en la ventana Añadir excepción de seguridad, pulse **Ver**.
   c. Pulse la pestaña **Detalles** y luego pulse **Exportar**.

d. En el campo **Nombre de archivo**, escriba `iemserver_cert.der`
e. En el campo **Guardar como tipo**, seleccione **Certificado X.509 (DER)** y pulse **Guardar**.
f. Copie el certificado de clave pública en la consola de QRadar.
g. Para crear un almacén de confianza de QRadar Vulnerability Manager, utilice SSH para iniciar una sesión en la consola de QRadar como usuario root.

   Escriba el mandato siguiente: `keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias iem`

   En los campos de solicitud, escriba la información adecuada para crear el almacén de claves de confianza.
h. Para importar el certificado de clave pública al almacén de claves de confianza, escriba el mandato siguiente:

   `keytool -importcert -file iemserver_cert.der -keystore truststore.jks -storepass <`*`contraseña_almacén_claves`*`> -alias iem_crt_der`
i. En el campo de solicitud **¿Confiar en este certificado?**, escriba **Sí**.

2. Para configurar SSL y el adaptador de BigFix para QRadar Vulnerability Manager, siga estos pasos.
   a. Utilice SSH para iniciar una sesión en la consola de QRadar como usuario root.
   b. Cambie de directorio a la ubicación siguiente:

      `/opt/qvm/iem`
   c. Especifique `./iem-setup-webreports.pl` y, cuando se le solicite, especifique la información para el servidor de BigFix.
   d. Si está utilizando SSL, en el campo de solicitud **¿Utilizar cifrado SSL?**, escriba la respuesta apropiada.
   e. Escriba la ubicación del almacén de confianza.
   f. Escriba la contraseña del almacén de confianza.

Configurar QRadar Vulnerability Manager para enviar información a BigFix

En esta opción de configuración, IBM Security QRadar Vulnerability Manager envía información a IBM BigFix. Esta opción de configuración exige diversos pasos de configuración para el adaptador de BigFix y algunos procedimientos de verificación.

Procedimiento

1. Inicie la sesión en el terminal de IBM Security QRadar SIEM como usuario root.
2. Para realizar la configuración, siga estos pasos:
   a. Vaya a `/opt/qvm/adaptor/config` y ejecute el script de configuración: `./setup-adaptor.sh`
   b. Especifique una contraseña nueva para crear el almacén de confianza, que es responsable de almacenar certificados.
   c. En las solicitudes, especifique la información adecuada para el servidor de BigFix.
   d. Reinicie el perfilador de activos accediendo al directorio `/opt/qradar/init` y tecleando el mandato siguiente: `./assetprofiler restart`

Para asegurar un rendimiento óptimo, no reinicie el perfilador de activos cuando se estén ejecutando exploraciones de QRadar Vulnerability Manager o cuando esté esperando importaciones de vulnerabilidad de un explorador de VIS de terceros.

3. Para comprobar que el proceso de configuración se ha realizado correctamente, siga estos pasos:
   a. En el archivo `/opt/qvm/adaptor/config/adaptor.properties`, compruebe que estas dos propiedades estén establecidas:

      ```
      qvm.adaptor.listener.enabled=true
      qvm.adaptor.process.daemon=false
      ```

   b. Establezca la puntuación de riesgo y la granularidad de actualización de activos mediante las propiedades siguientes en el archivo `adaptor.properties`:

Tabla 2.

Nombre de propiedad	Descripción
`qvm.adaptor.minimum.asset.riskscore=n`	La propiedad **`qvm.adaptor.minimum.asset.riskscore`** es la combinación ponderada de todas las puntuaciones de CVSS de las vulnerabilidades que se encuentran en el activo. Los activos que tienen una puntuación menor que este valor no se envían a BigFix.
`qvm.adaptor.assetupdate.limit=n`	La propiedad **`qvm.adaptor.assetupdate.limit`** define cómo se dividen los recursos de datos del Panel de instrumentos de BigFix. La división no se produce hasta que se llenan todos los IDs de CVE para el último activo. • Por ejemplo, si **`qvm.adaptor.assetupdate.limit=20`**, el activo 1 tiene 19 IDs de CVE y el activo 2 tiene 30 IDs de CVE. Se genera un recurso de datos que contiene ambos activos con un total de 49 IDs de CVE. • Por ejemplo, si **`qvm.adaptor.assetupdate.limit=19`**, el activo 1 tiene 19 IDs de CVE y el activo 2 tiene 30 IDs de CVE. Se generan dos recursos de datos que contienen cada uno un activo.
`qvm.adaptor.minimum.vuln.riskscore=n`	La propiedad **`qvm.adaptor.minimum.vuln.riskscore`** define el umbral para cada puntuación de riesgo de vulnerabilidad. Esas vulnerabilidades iguales o superior al valor establecido se envían a BigFix.

   c. Verifique que la configuración del plug-in BigFix ha creado los directorios siguientes:
      - `/store/qvm/adaptor`
      - `/store/qvm/adaptor/data`
      - `/store/qvm/adaptor/bigfix`

d. Verifique que el registro está habilitado en el archivo `log4j.xml`. Los archivos de registro se generan en los archivos `/var/log/qvm-integration-adaptor.log` y `/var/log/qvm-adaptor-cron.log`.

Resolución de problemas de la configuración de BigFix

Puede resolver los problemas de anomalía de conexión y restablecimiento de contraseña que pueden producirse al configurar la integración de BigFix y QRadar Vulnerability Manager.

Conexión anómala al servidor de IBM BigFix

Si se produce una conexión anómala al servidor de BigFix, puede que observe los errores siguientes:

```
ERROR [TrustStoreConfig] No se ha podido configurar el almacén de confianza con certificados del interlocutor:
Connection timed out java.net.ConnectException: Tiempo espera de conexión agotado.
```

La configuración es satisfactoria, pero no tendrá los certificados autorizados. Debe cargar manualmente los certificados cuando tenga acceso al servidor.

1. Vaya al directorio `/store/qvm/adaptor`.
2. Ejecute el script de configuración: `./install-cert.sh` *<ubicación_almacén_confianza>* *<contraseña_almacén_confianza>*<*dirección_IP_almacén_confianza: puerto*>
   El puerto es el puerto de servicio al que pertenece el certificado.

Cambio de contraseña

Si cambian los detalles de BigFix, puede que sea necesario cambiar la contraseña.

1. Descifre la contraseña especificando el mandato siguiente: `_decrypt.bes.rest.password=lUb5qzr7FIVH+J319erc+g==`.
2. Para escribir una contraseña nueva, especifique el mandato siguiente: `_encrypt.bes.rest.password=`*newpassword*.
3. Ejecute el script siguiente para cifrar la contraseña nueva: `./password-property-encrypt.sh plugin-bigfix.properties`

Integración de IBM Security SiteProtector

QRadar Vulnerability Manager se integra con IBM Security SiteProtector para ayudar a dirigir la política del sistema de prevención de intrusiones (IPS).

Cuando configura IBM Security SiteProtector, las vulnerabilidades detectadas por las exploraciones se reenvían automáticamente a SiteProtector.

IBM Security SiteProtector recibe datos de vulnerabilidad procedentes de las exploraciones realizadas de QRadar Vulnerability Manager solamente después de que la integración esté configurada.

Conexión con IBM Security SiteProtector

Puede reenviar datos de vulnerabilidad desde IBM Security QRadar Vulnerability Manager a IBM Security SiteProtector para ayudar a dirigir la política del sistema de prevención de intrusiones (IPS).

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
2. Pulse **Utilizar SiteProtector**.
3. En el campo **Dirección IP de SiteProtector**, escriba la dirección IP del servidor de IBM Security SiteProtector Agent Manager.
4. Pulse **Guardar** y, a continuación, pulse **Cerrar**.
5. En la barra de herramientas del panel **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
6. Pulse **Aceptar**.

Qué hacer a continuación

Explore los activos de red para determinar si los datos de vulnerabilidad se visualizan en la instalación de IBM Security SiteProtector.

Capítulo 5. Exploración de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, toda la exploración de la red está controlada por los perfiles de exploración creados por el usuario. Puede crear varios perfiles de exploración y configurar cada perfil de forma diferente de acuerdo con los requisitos específicos de la red.

Perfiles de exploración

Utilice perfiles de exploración para realizar las tareas siguientes:

- Especificar los nodos de red, dominios o dominios virtuales que desee explorar.
- Especificar los activos de red que desee excluir de las exploraciones.
- Crear intervalos operativos que definen el momento en que se pueden ejecutar las exploraciones.
- Ejecutar manualmente perfiles de exploración o planificar una exploración para que se ejecute en una fecha futura.
- Ejecutar, poner en pausa, reanudar, cancelar o suprimir una sola exploración o varias .
- Utilizar credenciales centralizadas para ejecutar los sistemas operativos Windows, UNIX o Linux.
- Explorar los activos de una búsqueda de activos guardada.

Conceptos relacionados:

"Conjuntos de credenciales centralizadas" en la página 45
Cuando ejecuta exploraciones autenticadas, puede utilizar una lista central de credenciales de inicio de sesión para los sistemas operativos Linux, UNIX o Windows. El administrador del sistema debe configurar la lista de credenciales.

Crear un perfil de exploración

En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para especificar cómo y cuándo se exploran los activos de la red para buscar vulnerabilidades.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Además, también puede configurar los siguientes valores opcionales.

   - Si ha añadido más exploradores al despliegue de QRadar Vulnerability Manager, seleccione un explorador en la lista **Servidor de exploración**. Este paso no es necesario si desea utilizar la exploración dinámica.
   - Para habilitar este perfil para la exploración a petición, pulse el recuadro de selección **Exploración a petición habilitada**.

     Al seleccionar esta opción, hace que el perfil esté disponible para su uso si desea desencadenar una exploración como respuesta a un suceso de regla

personalizada. También habilita la exploración de vulnerabilidades a petición mediante el menú contextual en la página Activos.

- Marcando el recuadro de selección **Selección dinámica de servidor**, puede elegir el explorador más adecuado que esté disponible. Asegúrese de definir los exploradores en la página **Administrativo** > **Exploradores**.

  Los perfiles de seguridad deben actualizarse con un dominio asociado. Las restricciones de nivel de dominio no se aplican hasta que los perfiles de seguridad se han actualizado y se han desplegado los cambios.
- Para explorar la red utilizando un conjunto predefinido de criterios exploración, seleccione un tipo de exploración en la lista **Políticas de exploración**.
- Si ha configurado credenciales centralizadas para activos, pulse la casilla **Utilizar credenciales centralizadas**. Para obtener más información, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

4. Pulse **Guardar**.

Conceptos relacionados:

"Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7
Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

"Políticas de exploración" en la página 60
Una política de exploración proporciona una ubicación central para configurar los requisitos específicos de exploración.

"Exploraciones de vulnerabilidades dinámicas" en la página 58
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración para utilizar determinados exploradores de vulnerabilidades con rangos de CIDR determinados de la red. Por ejemplo, los exploradores pueden tener acceso solamente a determinadas áreas de la red.

Tareas relacionadas:

"Asociar exploraciones de vulnerabilidades a rangos de CIDR" en la página 59
En IBM Security QRadar Vulnerability Manager, para realizar una exploración dinámica, debe asociar exploradores de vulnerabilidades a segmentos diferentes de la red.

"Reexploración de un activo mediante la opción del menú contextual" en la página 35
En IBM Security QRadar Vulnerability Manager, puede rápidamente explorar de nuevo un activo pulsando el botón derecho de ratón.

"Configurar una política de exploración para gestionar las exploraciones de vulnerabilidades" en la página 62
En IBM Security QRadar Vulnerability Manager, puede configurar una política de exploración para controlar las exploraciones de vulnerabilidades.

Crear un perfil de exploración de explorador externo

En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para utilizar un explorador alojado para explorar activos de la zona desmilitarizada de la red.

Antes de empezar

QRadar Vulnerability Manager se debe configurar con un explorador alojado. Para obtener más información, consulte "Explorar activos de la zona desmilitarizada" en la página 10.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para crear un perfil de explorador externo, también debe seguir los pasos restantes de este procedimiento.
4. Seleccione un explorador externo en la lista **Servidor de exploración**.
5. Seleccione **Exploración completa** o **Exploración de web** en la lista **Políticas de exploración**.
6. Pulse la pestaña **Dominio y aplicaciones web**. En el panel **Webs virtuales**, escriba el dominio y la dirección IP de los sitios web y aplicaciones que desee explorar.
7. Pulse **Guardar**.

   Nota: Las exploraciones autenticadas no se llevan a cabo desde el explorador externo.

Crear un perfil de referencia

Para crear exploraciones de conformidad de Center for Internet Security, debe configurar perfiles de referencia. Utilice las exploraciones de conformidad de CIS para verificar la conformidad de referencia de CIS para Windows y Red Hat Enterprise Linux.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir prueba de referencia**.
4. Si desea utilizar credenciales centralizadas predefinidas, seleccione la casilla **Utilizar credenciales centralizadas**.

   Las credenciales que se utilizan para explorar sistemas operativos Linux deben tener privilegios de usuario root. Las credenciales que se utilizan para explorar sistemas operativos Windows deben tener privilegios de administrador.
5. Si no utiliza la exploración dinámica, seleccione un explorador de QRadar Vulnerability Manager en la lista **Servidor de exploración**.
6. Para habilitar la exploración dinámica, pulse el recuadro de selección **Selección de servidor dinámica**.

   Si ha configurado dominios en la ventana **Admin** > **Gestión de dominios**, puede seleccionar un dominio de la lista **Dominio**. Solamente se exploran los activos incluidos en los rangos de CIDR y los dominios que están configurados para los exploradores.
7. En el panel **Cuándo explorar**, establezca la planificación de ejecución, la hora de inicio de la exploración y los intervalos operativos que haya predefinidos.
8. En el panel **Correo electrónico**, defina qué información se debe enviar referente a la exploración y a quién se debe enviar.
9. Si no utiliza credenciales centralizadas, añada las credenciales que la exploración necesite en el panel **Credenciales adicionales**.

Las credenciales que se utilizan para explorar sistemas operativos Linux deben tener privilegios de usuario root. Las credenciales que se utilizan para explorar sistemas operativos Windows deben tener privilegios de administrador.

10. Pulse **Guardar**.

Conceptos relacionados:

"Conjuntos de credenciales centralizadas" en la página 45
Cuando ejecuta exploraciones autenticadas, puede utilizar una lista central de credenciales de inicio de sesión para los sistemas operativos Linux, UNIX o Windows. El administrador del sistema debe configurar la lista de credenciales.

Ejecución manual de perfiles de exploración

En IBM Security QRadar Vulnerability Manager, puede ejecutar manualmente un perfil de exploración o varios.

Puede también planificar exploraciones para que se ejecuten en una fecha y hora futuras. Para obtener más información, consulte "Planificación de exploración" en la página 37.

Antes de empezar

Compruebe que haya un procesador de vulnerabilidades desplegado. Para obtener más información, consulte "Verificar que se ha desplegado un procesador de vulnerabilidades" en la página 7.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la página Perfiles de exploración, marque el recuadro de selección en la fila asignada al perfil de exploración que desea ejecutar.

   Nota: Para localizar los perfiles de exploración que desea ejecutar, utilice el campo **Nombre** de la barra de herramientas para filtrar los perfiles de exploración por nombre.
4. En la barra de herramientas, pulse **Ejecutar**.

   De forma predeterminada se realiza una exploración rápida utilizando el Protocolo de control de transmisiones (TCP) y el Protocolo de datagramas de usuario (UDP). Una exploración rápida comprende la mayoría de los puertos del rango 1 – 1024.

Conceptos relacionados:

"Detalles de perfil de exploración" en la página 35
En IBM Security QRadar Vulnerability Manager puede describir una exploración, seleccionar el explorador que desea utilizar y elegir entre varias opciones de política de exploración.

Tareas relacionadas:

"Gestionar resultados de exploración" en la página 67
En la página Resultados de exploración de IBM Security QRadar Vulnerability Manager, puede gestionar los resultados de exploración y las exploraciones que están en ejecución.

Reexploración de un activo mediante la opción del menú contextual

En IBM Security QRadar Vulnerability Manager, puede rápidamente explorar de nuevo un activo pulsando el botón derecho de ratón.

La opción de exploración con el botón derecho del ratón también está disponible en la pestaña Delitos de QRadar y en la vista de activos de subred de QRadar Risk Manager.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Gestionar vulnerabilidades** > **Por activo**.
3. En la página Por activo, identifique el activo que desee volver a explorar.
4. Pulse con el botón derecho del ratón en **Dirección IP** y seleccione **Ejecutar Exploración de vulnerabilidad**.
5. En la ventana Ejecutar Exploración de vulnerabilidad, seleccione el perfil de exploración que desee utilizar cuando se explore de nuevo el activo.

   El proceso de exploración necesita un perfil de exploración. El perfil de exploración determina las opciones de configuración de exploración que se utilizan cuando se ejecuta la exploración.

   Para ver un perfil de exploración en la ventana Ejecutar Exploración de vulnerabilidad, debe marcar el recuadro de selección **Exploración a petición habilitada** de la pestaña **Detalles** en la página Configuración de perfil de exploración.

   Importante: El perfil de exploración que seleccione puede estar asociado a varios destinos de exploración o rangos de direcciones IP. Pero cuando ejecuta la exploración mediante el botón derecho del ratón, solo se explora el activo seleccionado.
6. Pulse **Explorar ahora**.
7. Pulse **Cerrar ventana**.
8. Para revisar el progreso de la exploración, pulse **Resultados de exploración** en el panel de navegación.

   Las exploraciones realizadas mediante el botón derecho de ratón se identifican mediante el prefijo **RC:**.

Conceptos relacionados:

"Vulnerabilidades de activos" en la página 79
En IBM Security QRadar Vulnerability Manager, puede visualizar datos de vulnerabilidad de resumen que están agrupados para cada activo explorado.

Detalles de perfil de exploración

En IBM Security QRadar Vulnerability Manager puede describir una exploración, seleccionar el explorador que desea utilizar y elegir entre varias opciones de política de exploración.

Los detalles del perfil de exploración se especifican en el panel **Detalles** de la página Configuración de perfil de exploración.

Consulte especialmente las opciones siguientes:

Tabla 3. Opciones de configuración de los detalles del perfil de exploración

Opciones	Descripción
Utilizar credenciales centralizadas	Especifica que el perfil utiliza credenciales predefinidas. Las credenciales centralizadas se definen en la ventana **Admin** > **Configuración del sistema** > **Credenciales centralizadas**.
Servidor de exploración	El explorador que seleccione depende de la configuración de red. Por ejemplo, para explorar activos de DMZ (zona desmilitarizada), seleccione un explorador que tenga acceso a esa zona de la red. El servidor de exploración de **Controlador** se despliega con el procesador de vulnerabilidades en la consola de QRadar o en un host gestionado de QRadar Vulnerability Manager. **Restricción:** Puede tener un solo procesador de vulnerabilidades en el despliegue. Pero puede desplegar varios exploradores, ya sea en dispositivos exploradores dedicados de host gestionado de QRadar Vulnerability Manager o en hosts gestionados de QRadar.
Exploración a petición	Habilita la exploración de activos a petición para el perfil. Utilice el menú contextual en la página Activos para que se ejecute la exploración de vulnerabilidades a petición. Al seleccionar esta opción, también hace que el perfil esté disponible para su uso si desea desencadenar una exploración como respuesta a un suceso de regla personalizada. Al habilitar la exploración a petición, también puede habilitar la exploración dinámica.
Selección de servidor dinámica	Especifica si desea utilizar un explorador de vulnerabilidades separado para cada rango de CIDR que desee explorar. Durante una exploración, QRadar Vulnerability Manager asigna automáticamente la actividad de exploración al explorador correcto para cada rango de CIDR que especifique. Si ha configurado dominios en la ventana Gestión de dominios de la pestaña **Admin**, también puede seleccionar el dominio que desea explorar.
Límite de ancho de banda	Es el ancho de banda de la exploración. El valor predeterminado es medio. **Importante:** Si selecciona un valor mayor que 1000 kbps, puede afectar al rendimiento de la red.
Políticas de exploración	Son los criterios de exploración preconfigurados sobre puertos y protocolos. Para obtener más información, consulte “Políticas de exploración” en la página 60.

Conceptos relacionados:

“Exploraciones de vulnerabilidades dinámicas” en la página 58
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración para utilizar determinados exploradores de vulnerabilidades con rangos de CIDR determinados de la red. Por ejemplo, los exploradores pueden tener acceso solamente a determinadas áreas de la red.

“Políticas de exploración” en la página 60
Una política de exploración proporciona una ubicación central para configurar los requisitos específicos de exploración.

Planificación de exploración

En IBM Security QRadar Vulnerability Manager, puede planificar las fechas y horas en que es conveniente explorar los activos de red para buscar vulnerabilidades conocidas.

La planificación de exploración se controla mediante el panel **Cuándo explorar** de la página Configuración de perfil de exploración.

Un perfil de exploración que se ha configurado con un valor manual se debe ejecutar manualmente. Pero los perfiles de exploración que no están configurados como exploraciones manuales, también se pueden ejecutar manualmente.

Cuando selecciona una planificación de exploración, puede refinar más la planificación configurando un intervalo de exploración permitida.

Tareas relacionadas:

"Configurar un intervalo de exploración permitida" en la página 56
En IBM Security QRadar Vulnerability Manager, puede crear un intervalo operativo para especificar el momento en que se puede ejecutar una exploración.

"Revisar las exploraciones planificadas en formato de calendario" en la página 39
En IBM Security QRadar Vulnerability Manager, el calendario de exploraciones planificadas proporciona un lugar central donde puede revisar información sobre exploraciones planificadas.

Explorar dominios mensualmente

En IBM Security QRadar Vulnerability Manager, puede configurar un perfil de exploración para explorar los dominios de la red cada mes.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para configurar exploraciones mensuales, también debe seguir los pasos restantes de este procedimiento.
4. Pulse el panel **Cuándo explorar**.
5. En la lista **Ejecutar planificación**, seleccione **Mensualmente**.
6. En el campo **Hora de inicio**, seleccione una fecha y hora de inicio para la exploración.
7. En el campo **Día del mes**, seleccione un día para cada mes que se ejecuta la exploración.
8. Pulse la pestaña **Dominio y aplicaciones web**.
9. En el campo **Dominios**, escriba el URL del activo que desee explorar y pulse (>).
10. Pulse **Guardar**.
11. Opcional: Durante y después de la exploración, puede supervisar el progreso de la exploración y revisar las exploraciones completadas.

Planificar exploraciones de activos nuevos no explorados

En IBM Security QRadar Vulnerability Manager, puede configurar exploraciones planificadas de activos de red recién descubiertos, no explorados.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activos**, y en la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
3. Para especificar activos recién descubiertos, no explorados, siga los pasos siguientes en el panel **Parámetros de búsqueda**:
   a. Seleccione **Días desde que se encontró el activo**, **Menos de 2** y luego pulse **Añadir filtro**.
   b. Seleccione **Días desde que se exploró el activo Más de 2** y luego pulse **Añadir filtro**.
   c. Pulse **Buscar**.
4. En la barra de herramientas, pulse **Guardar criterios** y siga los pasos siguientes:
   a. En el campo **Especifique el nombre de esta búsqueda**, escriba el nombre de la búsqueda de activos.
   b. Pulse **Incluir en Búsquedas rápidas**.
   c. Pulse **Compartir con todos**.
   d. Pulse **Aceptar**.
5. Pulse la pestaña **Vulnerabilidades**.
6. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
7. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para planificar exploraciones de activos no explorados, también debe seguir los pasos restantes de este procedimiento.
8. En el panel Incluir búsquedas guardadas, seleccione la búsqueda de activos guardada en la lista **Búsquedas guardadas disponibles** y pulse (>).
9. Pulse el panel **Cuándo explorar** y seleccione **Semanalmente** en la lista **Ejecutar planificación**.
10. En los campos **Hora de inicio**, escriba o seleccione la fecha y hora en que desee que se ejecute la exploración en cada día seleccionado de la semana.
11. Seleccione las casillas correspondientes a los días de la semana en que desee que se ejecute la exploración.
12. Pulse **Guardar**.

    Para obtener más información sobre el uso de la pestaña **Activos** y cómo guardar búsquedas de activos, consulte la *Guía del usuario* del producto.

Tareas relacionadas:

"Buscar datos de vulnerabilidad" en la página 72
En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

Revisar las exploraciones planificadas en formato de calendario

En IBM Security QRadar Vulnerability Manager, el calendario de exploraciones planificadas proporciona un lugar central donde puede revisar información sobre exploraciones planificadas.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Exploraciones planificadas**.
3. Opcional: Pase el cursor del ratón sobre la exploración planificada para mostrar información sobre ella.

   Por ejemplo, puede mostrar el tiempo que una exploración tardó en completarse.
4. Opcional: Haga una doble pulsación sobre una exploración planificada para editar el perfil de exploración.

Destinos y exclusiones de la exploración de red

En IBM Security QRadar Vulnerability Manager, puede proporcionar información sobre los activos, dominios o webs virtuales de la red que desee explorar.

Utilice la pestaña **Detalles** de la página Configuración del perfil de exploración para especificar los activos de red que desee explorar.

Puede excluir un host o rango de hosts determinado que no se debe explorar nunca. Por ejemplo, puede impedir que una exploración se ejecute en servidores críticos donde se alojan aplicaciones de producción. Puede también configurar la exploración para que se realice solamente en áreas determinadas de la red.

QRadar Vulnerability Manager se integra con QRadar mediante la opción para explorar los activos que forman parte de una búsqueda de activos guardada.

Destinos de exploración

Puede especificar destinos de exploración definiendo un rango de CIDR, una dirección IP, un rango de direcciones IP o una combinación de todos ellos.

Exploración de dominios

Puede añadir dominios al perfil de exploración para comprobar si hay transferencias de zona de DNS en cada uno de los dominios que especifique.

Un host puede utilizar la transferencia de zona de DNS para solicitar y recibir una transferencia de zona completa para un dominio. La transferencia de zona es un problema de seguridad porque los datos de DNS se utilizan para descifrar la topología de la red. Los datos que están contenidos en una transferencia de zona de DNS son confidenciales y por lo tanto cualquier exposición de los datos se podría percibir como una vulnerabilidad. La información obtenida se podría utilizar para una explotación maliciosa, tal como el envenenamiento de DNS o la suplantación de identidades.

Exploraciones que utilizan búsquedas de activos guardadas

Puede explorar los activos y las direcciones IP que están asociados a una búsqueda de activos guardada de QRadar.

Las búsquedas guardadas se muestran en la sección **Búsqueda guardada de activos** de la pestaña **Detalles**.

Para obtener más información sobre cómo guardar búsquedas de activos, consulte la *Guía del usuario* del producto.

Excluir destinos de exploración de red

En la sección **Activos excluidos** de la pestaña **Dominio y aplicaciones web**, puede especificar las direcciones IP, rangos de direcciones IP o rangos de CIDR para los activos que no deben explorarse. Por ejemplo, si desea impedir que se explore un servidor muy cargado, inestable o con información confidencial, excluya estos activos.

Cuando configura una exclusión de exploración en una configuración de perfil de exploración, la exclusión se aplica sólo al perfil de exploración.

Webs virtuales

Puede configurar un perfil de exploración para explorar diferentes URL que están alojados en la misma dirección IP.

Cuando analiza una web virtual, QRadar Vulnerability Manager comprueba si hay inyección de SQL y vulnerabilidades de script entre sitios en cada página web.

Tareas relacionadas:

"Explorar rangos de CIDR con exploradores de vulnerabilidades diferentes" en la página 60
En IBM Security QRadar Vulnerability Manager, puede explorar áreas de una red con diferentes exploradores de vulnerabilidades.

"Excluir activos en todas las exploraciones"
En IBM Security QRadar Vulnerability Manager, las exclusiones de exploración especifican los activos de la red que no se exploran.

"Planificar exploraciones de activos nuevos no explorados" en la página 38
En IBM Security QRadar Vulnerability Manager, puede configurar exploraciones planificadas de activos de red recién descubiertos, no explorados.

"Explorar dominios mensualmente" en la página 37
En IBM Security QRadar Vulnerability Manager, puede configurar un perfil de exploración para explorar los dominios de la red cada mes.

Excluir activos en todas las exploraciones

En IBM Security QRadar Vulnerability Manager, las exclusiones de exploración especifican los activos de la red que no se exploran.

Acerca de esta tarea

Las exclusiones de exploración se aplican a todas las configuraciones del perfil de exploración y se pueden utilizar para excluir la actividad de exploración en los servidores inestables o que contienen información confidencial. Utilice el campo **Direcciones IP** de la página Exclusión de exploración para especificar las

direcciones IP, rangos de direcciones IP o rangos de CIDR que desea excluir de toda exploración. Para acceder a la página Exclusión de exploración:

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Exclusiones de exploración**.
3. En la barra de herramientas, seleccione **Acciones** > **Añadir**.

   Nota: También puede utilizar la sección **Activos excluidos** de la pestaña **Vulnerabilidades** > **Administrativo** > **Perfiles de exploración** > **Añadir** > **Dominio y aplicaciones web** para excluir activos de un perfil de exploración en concreto.

Gestionar exclusiones de exploración

En IBM Security QRadar Vulnerability Manager, puede actualizar, suprimir o visualizar exclusiones de exploración.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Exclusiones de exploración**.
3. En la lista de la página Exclusiones de exploración, pulse la **Exclusión de exploración** que desee modificar.
4. En la barra de herramientas, seleccione una opción del menú **Acciones**.
5. Dependiendo de la selección que realice, siga las instrucciones de la pantalla para completar esta tarea.

Protocolos y puertos de exploración

En IBM Security QRadar Vulnerability Manager, puede elegir diferentes protocolos de exploración y explorar diversos rangos de puertos.

Utilice el panel **Cómo explorar** de la página Configuración del perfil de exploración para especificar protocolos de exploración y los puertos que desee explorar.

Utilice las opciones siguientes para configurar los protocolos de puertos del perfil de exploración:

Tabla 4. Opciones para protocolos y puertos de exploración

Protocolo	Descripción
TCP y UDP	Protocolo de exploración predeterminado que explora los puertos comunes comprendidos en el rango 1 - 1024. **Recuerde:** En comparación con otros protocolos de exploración, TCP y UDP pueden generar más actividad de red.
TCP	Es el protocolo de exploración más habitual. Cuando la exploración TCP se combina con la exploración de rangos de IP, puede localizar un host donde se ejecutan servicios que son propensos a vulnerabilidades. El rango de puertos predeterminado es 1 - 65535.

Tabla 4. Opciones para protocolos y puertos de exploración (continuación)

Protocolo	Descripción
SYN	Envía un paquete a todos los puertos especificados. Si el puerto de destino está a la escucha, el puerto responde con un carácter de sincronización (SYN) y un carácter de acuse de recibo (ACK). Si el puerto de destino no está a la escucha, el puerto responde con una señal de restauración (RST). Normalmente, se cierra el puerto de destino y se devuelve una señal RST. El rango de puertos predeterminado es 1 - 65535.
ACK	Es similar a SYN, pero en este caso se activa un distintivo de acuse de recibo (ACK). La exploración de ACK no determina si el puerto está abierto o cerrado, sino que comprueba si el puerto está filtrado o no filtrado. La comprobación del puerto es útil para detectar la existencia de un cortafuegos y sus conjuntos de reglas. El filtrado de paquetes simple habilita el establecimiento de conexiones (paquetes con el bit ACK activado), mientras que un cortafuegos con estados más complejo podría no hacerlo. El rango de puertos predeterminado es 1-65535.
FIN	Paquete TCP que se utiliza para cerrar una conexión, o se puede utilizar como método para identificar puertos abiertos. FIN envía paquetes erróneos a un puerto y espera que los puertos abiertos que están a la escucha devuelvan mensajes de error diferentes que los enviados por puertos cerrados. El explorador envía un paquete FIN, el cual podría cerrar una conexión que está abierta. Los puertos cerrados responden a un paquete FIN con una señal RST. Los puertos abiertos pasan por alto el paquete en cuestión. El rango de puertos predeterminado es 1 - 65535.

Explorar un rango de puertos completo

En IBM Security QRadar Vulnerability Manager, puede explorar el rango de puertos completo en los activos que especifique.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para explorar un rango de puertos completo, también debe seguir los pasos restantes de este procedimiento.
4. Pulse la pestaña **Cómo explorar**.
5. En el campo **Protocolo**, acepte los valores predeterminados **TCP y UDP**.
6. En el campo **Rango**, escriba **1-65535**.

   Restricción: Los rangos de puertos se deben especificar en orden ascendente consecutivo, separados por guiones y delimitados por comas, y sin solapamientos. Se especifica varios rangos de puertos, debe separarlos con una coma. Los ejemplos siguientes muestran los delimitadores que se utilizan para especificar rangos de puertos: (1-1024, 1055, 2000-65535).
7. En el campo **Tiempo de espera (m)**, escriba el número de minutos transcurridos los cuales se debe cancelar la exploración si no se descubre ningún resultado de exploración.

Importante: Puede escribir un valor cualquiera comprendido dentro del rango 1 - 500. No especifique un tiempo demasiado corto, pues la exploración de puertos no podría detectar todos los puertos abiertos. Se mostrarán los resultados de exploración que se han descubierto antes de que termine el periodo de tiempo de espera.

8. Pulse **Guardar**.
9. En la página Perfiles de exploración, pulse **Ejecutar**.

Explorar activos con puertos abiertos

En IBM Security QRadar Vulnerability Manager, puede configurar un perfil de exploración para explorar activos con puertos abiertos.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activos**, y en la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
3. Para especificar activos con puertos abiertos, configure las opciones siguientes en el panel **Parámetros de búsqueda**:
   a. Seleccione **Activos con puerto abierto**, **Es igual a cualquiera de 80** y pulse **Añadir filtro**.
   b. Seleccione **Activos con puerto abierto**, **Es igual a cualquiera de 8080** y pulse **Añadir filtro**.
   c. Pulse **Buscar**.
4. En la barra de herramientas, pulse **Guardar criterios** y configure las opciones siguientes:
   a. En el campo **Especifique el nombre de esta búsqueda**, escriba el nombre de la búsqueda de activos.
   b. Pulse **Incluir en Búsquedas rápidas**.
   c. Pulse **Compartir con todos** y luego pulse **Aceptar**.
5. Pulse la pestaña **Vulnerabilidades**.
6. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
7. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para explorar activos con puertos abiertos, también debe seguir los pasos restantes de este procedimiento.
8. En la pestaña **Detalles**, seleccione la búsqueda de activos guardada en la lista **Búsquedas guardadas disponibles** y pulse **>**.

   Cuando incluye una búsqueda de activos guardada en el perfil de exploración, se exploran los activos y las direcciones IP asociados a la búsqueda guardada.
9. Pulse el panel **Cuándo explorar** y seleccione **Manual** en la lista **Ejecutar planificación**.
10. Pulse el panel **Qué explorar**.
11. Pulse **Guardar**.

    Para obtener más información sobre cómo guardar búsquedas de activos, consulte la *Guía del usuario* del producto.

Qué hacer a continuación

Siga los pasos que se indican en el procedimiento, "Ejecución manual de perfiles de exploración" en la página 34.

Exploraciones de parches autenticadas

En IBM Security QRadar Vulnerability Manager, puede buscar nombres de comunidad y ejecutar exploraciones de parches autenticadas para los sistemas operativos Windows, Linux y UNIX.

Nombres de comunidad SNMP

Puede explorar los activos de la red utilizando nombres de comunidad SNMP.

Cuando se exploran activos, QRadar Vulnerability Manager realiza la autenticación utilizando los servicios SNMP encontrados y realiza una exploración de vulnerabilidades más detallada.

Exploraciones de parches en Windows

Para explorar sistemas operativos Windows en búsqueda de parches que faltan, se debe habilitar el acceso al Registro y la interfaz de gestión de Windows (WMI). Si la exploración de parches de Windows devuelve los problemas de conectividad de WMI, debe configurar los sistemas Windows.

Para leer datos de WMI en un servidor remoto, debe habilitar las conexiones entre la consola de QRadar y el servidor que está supervisando. Si el servidor está utilizando un cortafuegos de Windows, debe configurar el sistema para habilitar solicitudes de WMI remotas.

Si utiliza una cuenta no administrativa para supervisar el servidor Windows, debe habilitar la cuenta para interactuar con el Modelo de objetos componentes distribuido (DCOM).

Si la herramienta de exploración de parches no se puede conectar a un activo de Windows, se muestra un icono de aviso en forma de triángulo amarillo junto al activo en los resultados de exploración. Se emite la vulnerabilidad siguiente: `Local Checks Error`.

Exploración autenticada segura del sistema operativo Linux

Para explorar sistemas operativos Linux utilizando la autenticación segura, puede configurar el cifrado de clave pública entre la consola o el host gestionado y los destinos de exploración.

Cuando está configurada la autenticación segura, no necesita especificar una contraseña del sistema operativo Linux en el perfil de exploración.

Debe configurar la autenticación de clave pública en cada sistema operativo Linux que desee explorar.

Si traslada el procesador de vulnerabilidades a un dispositivo procesador de vulnerabilidades dedicado, debe volver a configurar la autenticación segura entre el procesador de vulnerabilidades dedicado y el destino de exploración.

Si la herramienta de exploración de parches no se puede conectar a un activo de Linux, se muestra un icono de aviso en forma de triángulo amarillo junto al activo en los resultados de exploración. Se emite la vulnerabilidad siguiente: `SSH Patch Scanning - Failed Logon`.

Tareas relacionadas:

"Configurar la autenticación de clave pública del sistema operativo Linux" en la página 46
Para explorar sistemas operativos Linux utilizando la autenticación de clave pública segura, debe configurar la consola o host gestionado de IBM Security QRadar y el activo que desee explorar. Cuando la autenticación está configurada, puede realizar una exploración autenticada especificando un nombre de usuario del sistema operativo Linux, sin especificar una contraseña. QRadar soporta `rsa` y `dsa` para la generación de claves SSH.

"Configurar una exploración autenticada de los sistemas operativos Linux o UNIX" en la página 47
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de autenticación de los sistemas operativos Linux o UNIX que residen en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

"Configurar una exploración autenticada del sistema operativo Windows" en la página 49
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de los sistemas operativos Windows que están instalados en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

Conjuntos de credenciales centralizadas

Cuando ejecuta exploraciones autenticadas, puede utilizar una lista central de credenciales de inicio de sesión para los sistemas operativos Linux, UNIX o Windows. El administrador del sistema debe configurar la lista de credenciales.

Un administrador puede especificar credenciales para dispositivos de red SNMP y para los sistemas operativos Linux, UNIX o Windows. Por lo tanto, el usuario encargado de configurar un perfil de exploración no necesita conocer las credenciales de cada activo explorado. Además, si cambian las credenciales de un activo, las credenciales se pueden modificar centralmente, en lugar de actualizar el perfil de exploración.

Tareas relacionadas:

"Configurar una exploración autenticada de los sistemas operativos Linux o UNIX" en la página 47
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de autenticación de los sistemas operativos Linux o UNIX que residen en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

"Configurar una exploración autenticada del sistema operativo Windows" en la página 49
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de los sistemas operativos Windows que están instalados en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

"Crear un perfil de referencia" en la página 33
Para crear exploraciones de conformidad de Center for Internet Security, debe configurar perfiles de referencia. Utilice las exploraciones de conformidad de CIS para verificar la conformidad de referencia de CIS para Windows y Red Hat Enterprise Linux.

Configurar un conjunto de credenciales

En IBM Security QRadar Vulnerability Manager, puede crear un conjunto de credenciales para los activos de la red. Durante una exploración, si una herramienta de exploración necesita las credenciales de un sistema operativo Linux, UNIX o Windows, las credenciales se pasan automáticamente a la herramienta de exploración desde el conjunto de credenciales.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel **Configuración del sistema**, pulse **Credenciales centralizadas**.
3. En la barra de herramientas de la ventana Credenciales centralizadas, pulse **Añadir**.

   Para configurar un conjunto de credenciales, el único campo obligatorio de la ventana Conjunto de credenciales es el campo **Nombre**.
4. En la ventana Conjunto de credenciales, pulse la pestaña **Activos**.
5. Escriba un rango de CIDR para los activos para los que desee especificar credenciales y pulse **Añadir**.

   Los usuarios deben tener permisos de acceso de red otorgados en su perfil de seguridad para un rango de direcciones IP o CIDR que utilizan o para las que crean credenciales en **Credenciales centralizadas**.
6. Opcional: Pulse las pestañas **Linux/Unix, Windows, o Dispositivos de red (SNMP)** cuando escriba las credenciales.
7. Pulse **Guardar**.

Configurar la autenticación de clave pública del sistema operativo Linux

Para explorar sistemas operativos Linux utilizando la autenticación de clave pública segura, debe configurar la consola o host gestionado de IBM Security QRadar y el activo que desee explorar. Cuando la autenticación está configurada, puede realizar una exploración autenticada especificando un nombre de usuario del sistema operativo Linux, sin especificar una contraseña. QRadar soporta `rsa` y `dsa` para la generación de claves SSH.

Antes de empezar

Debe configurar la clave pública en el dispositivo donde está instalado el procesador de vulnerabilidades. Para obtener más información, consulte "Verificar que se ha desplegado un procesador de vulnerabilidades" en la página 7.

Procedimiento

1. Mediante SSH, inicie una sesión en la consola o host gestionado de QRadar como usuario root.
2. Genere un par de claves públicas DSA escribiendo el mandato siguiente:

   ```
   su -m -c 'ssh-keygen -t dsa' qvmuser
   ```
3. Acepte el archivo predeterminado pulsando **Intro**.

4. Acepte la frase de contraseña predeterminada para la clave DSA pulsando la tecla **Intro**.
5. Pulse la tecla **Intro** de nuevo para confirmarla.
6. Copie la clave pública en el destino de exploración escribiendo el mandato siguiente:

   ```
   ssh-copy-id -i /home/qvmuser/.ssh/id_dsa.pub root@<dirección_IP>
   ```

   Cambie <*dirección_IP*> por la dirección IP del destino de exploración.
7. Escriba la frase de contraseña correspondiente al destino de exploración.
8. Compruebe que la cuenta de *qvmuser* en la consola puede utilizar SSH con el destino de exploración sin una frase de contraseña; para ello, escriba el mandato siguiente:

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no root@<dirección_IP> ls'
   qvmuser
   ```

   Cambie <*dirección_IP*> por la dirección IP del destino de exploración.

   Se visualiza una lista de los archivos en el directorio inicial del usuario root en el destino de exploración.

Qué hacer a continuación

Cree un perfil de exploración en QRadar Vulnerability Manager con el nombre de usuario *root* sin especificar una contraseña y ejecute una exploración de parche.

Tareas relacionadas:

"Configurar una exploración autenticada de los sistemas operativos Linux o UNIX"
En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de autenticación de los sistemas operativos Linux o UNIX que residen en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

Configurar una exploración autenticada de los sistemas operativos Linux o UNIX

En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de autenticación de los sistemas operativos Linux o UNIX que residen en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

Antes de empezar

Para realizar una exploración utilizando una lista de credenciales, debe primero definir una lista central de las credenciales que son necesarias para los sistemas operativos. Para obtener más información, consulte "Configurar un conjunto de credenciales" en la página 46.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración

del perfil de exploración. Para configurar una exploración autenticada, también debe seguir los pasos restantes de este procedimiento.

4. Opcional: Pulse **Utilizar credenciales centralizadas** para explorar sistemas operativos Linux o UNIX.

   Si no existe un conjunto de credenciales configurado y no especifica manualmente las credenciales, las herramientas de exploración se ejecutan, pero no reciben credenciales.

   Si existe un conjunto de credenciales para los hosts que está explorando, las credenciales que especifique manualmente en la pestaña **Credenciales adicionales** prevalecen sobre el conjunto de credenciales.
5. Pulse la pestaña **Cuándo explorar**.
6. En la lista **Ejecutar planificación**, seleccione **Manual**.
7. Pulse la pestaña **Credenciales adicionales**.
8. En el área **Exploración de parches de Linux/Unix**, escriba el nombre de usuario y la contraseña para los hosts de Linux o UNIX que desee explorar y pulse >.

   No es necesaria una contraseña si ha configurado la autenticación por clave pública segura entre la consola y el destino de exploración.
9. Pulse **Guardar**.
10. En la página Perfiles de exploración, pulse **Ejecutar**.

Conceptos relacionados:

"Conjuntos de credenciales centralizadas" en la página 45
Cuando ejecuta exploraciones autenticadas, puede utilizar una lista central de credenciales de inicio de sesión para los sistemas operativos Linux, UNIX o Windows. El administrador del sistema debe configurar la lista de credenciales.

Tareas relacionadas:

"Configurar un conjunto de credenciales" en la página 46
En IBM Security QRadar Vulnerability Manager, puede crear un conjunto de credenciales para los activos de la red. Durante una exploración, si una herramienta de exploración necesita las credenciales de un sistema operativo Linux, UNIX o Windows, las credenciales se pasan automáticamente a la herramienta de exploración desde el conjunto de credenciales.

"Configurar la autenticación de clave pública del sistema operativo Linux" en la página 46
Para explorar sistemas operativos Linux utilizando la autenticación de clave pública segura, debe configurar la consola o host gestionado de IBM Security QRadar y el activo que desee explorar. Cuando la autenticación está configurada, puede realizar una exploración autenticada especificando un nombre de usuario del sistema operativo Linux, sin especificar una contraseña. QRadar soporta `rsa` y `dsa` para la generación de claves SSH.

Habilitación de permisos para exploración de parches de Linux o UNIX

Las cuentas de usuario no root deben tener los permisos para ejecutar los mandatos que QRadar Vulnerability Manager necesita para explorar en busca de parches en sistemas Linux y UNIX.

Acerca de esta tarea

Para asignar los permisos relevantes para la exploración de parches de Linux o UNIX, utilice el procedimiento siguiente:

Procedimiento

1. SSH al activo.
2. Ejecute los mandatos siguientes `uname`:

```
uname -m
uname -n
uname -s
uname -r
uname -v
uname -p
uname -a
```

3. En función del sistema operativo, ejecute los mandatos siguientes:

Sistema operativo	Mandatos

Linux	Ejecute el contenido de los archivos siguientes que son relevantes para su distribución:
	1. /etc/redhat-release
	2. /etc/SuSE-release
	3. /etc/debian-version
	4. /etc/slackware-version
	5. /etc/mandrake-version
	6. /etc/gentoo-version
	Por ejemplo, en Red Hat Enterprise Linux, utilice los mandatos:
	`ls /etc/redhat-releasecat`
	`/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}`
	`|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Solaris	`/usr/bin/svcs -a`
	`/usr/bin/pkginfo -x | awk '{ if ( NR % 2 ) { prev = \$1 }`
	`else { print prev\" \"\$0 } }'`
	`/usr/bin/showrev -p`
	`/usr/sbin/patchadd -p`
	`/usr/bin/isainfo -b`
	`/usr/bin/isainfo -k`
	`/usr/bin/isainfo -n`
	`/usr/bin/isainfo -v`

HP-UX	`/usr/sbin/swlist -l fileset -a revision` `/usr/sbin/swlist -l patch`
AIX	`oslevel -r` `lslpp -Lc`
ESX	`vmware -vesxupdate query --all` `. /etc/profile ; /sbin/esxupdate query –all`

Configurar una exploración autenticada del sistema operativo Windows

En IBM Security QRadar Vulnerability Manager, puede configurar una exploración de los sistemas operativos Windows que están instalados en la red. Puede especificar manualmente las credenciales en el perfil de exploración o utilizar un conjunto de credenciales.

Si la exploración se realiza sin privilegios administrativos, QRadar Vulnerability Manager explora el registro remoto para cada instalación en el sistema operativo Windows.

La exploración sin privilegios administrativos es incompleta, propensa a producir falsos positivos y no abarca muchas aplicaciones externas.

Antes de empezar

QRadar Vulnerability Manager utiliza protocolos estándar de acceso remoto del sistema operativo Windows que están habilitados de forma predeterminada en la mayoría de los despliegues de Windows.

Si los resultados de la exploración de Windows devuelven una vulnerabilidad que indica problemas de conectividad de la interfaz de gestión de Windows (WMI), debe configurar los sistemas Windows.

Para obtener más información sobre la conectividad de Windows, consulte:

- "Habilitar el acceso remoto al Registro en el sistema operativo Windows" en la página 52.
- "Configuración de Windows Management Instrumentation" en la página 52.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para configurar una exploración autenticada del sistema operativo Windows, también debe seguir los pasos restantes de este procedimiento.
4. Opcional: Pulse **Utilizar credenciales centralizadas** para explorar sistemas operativos Windows.

   Debe configurar un conjunto de credenciales o especificar credenciales manualmente para los hosts para que las herramientas de exploración que requieren credenciales puedan ejecutarse.

   Si existe un conjunto de credenciales para los hosts que está explorando, las credenciales que especifique manualmente en la pestaña **Credenciales adicionales** prevalecen sobre el conjunto de credenciales.
5. Pulse el panel **Cuándo explorar**.
6. En la lista **Ejecutar planificación**, seleccione **Manual**.
7. Pulse el área **Credenciales adicionales**.
8. En el área **Exploración de parches de Windows**, escriba el **Dominio**, **Nombre de usuario** y **Contraseña** para los hosts de Windows que desee explorar y pulse (>).
9. Pulse **Guardar**.
10. En la página Perfiles de exploración, pulse **Ejecutar**.

Conceptos relacionados:

"Conjuntos de credenciales centralizadas" en la página 45
Cuando ejecuta exploraciones autenticadas, puede utilizar una lista central de credenciales de inicio de sesión para los sistemas operativos Linux, UNIX o

Windows. El administrador del sistema debe configurar la lista de credenciales.

"Exploraciones de parches autenticadas" en la página 44
En IBM Security QRadar Vulnerability Manager, puede buscar nombres de comunidad y ejecutar exploraciones de parches autenticadas para los sistemas operativos Windows, Linux y UNIX.

Exploración de parches de Windows

La *exploración de parches de Windows* es un método basado en red autenticado que se utiliza para preguntar al sistema de destino por la existencia de parches y actualizaciones faltantes relacionados con la seguridad.

La exploración de parches de Windows necesita acceso a 3 servicios clave de Windows:

- Registro remoto
- WMI
- Recursos compartidos administrativos

Es posible explorar sistemas en busca de parches de Windows sin utilizar WMI y Recursos compartidos administrativos pero los resultados no son completos y son propensos a proporcionar positivos falsos.

Utilice contraseñas complejas. Sin embargo, algunos caracteres especiales pueden provocar problemas. Limite los caracteres especiales a números, puntos, dos puntos, punto y coma, apóstrofos, signos de porcentaje y espacios.

Registro remoto

El servicio Registro remoto debe estar habilitado e iniciado y debe ser accesible desde el dispositivo de escáner de QRadar Vulnerability Manager y el usuario de exploración configurado utilizado en el perfil de exploración.

Si no es posible acceder al registro remoto, la exploración de parches de Windows falla completamente.

Si QRadar Vulnerability Manager no puede acceder al registro remoto, los resultados de la exploración registra el error siguiente:

```
Error de comprobaciones locales – El servicio del registro remoto no se
está ejecutando
```

en QRadar Vulnerability Manager versión 7.2.3 y posteriores, se visualiza un icono de triángulo amarillo junto al activo en los resultados de la exploración.

El estado del servicio de registro remoto se puede verificar en el **Panel de control administrativo**, bajo **Servicios**. Asegúrese de que los servicios dependientes siguientes están iniciados:

- Llamada a procedimiento remoto (RPC)
- Lanzador de proceso de servidor DCOM
- RPC EndPoint Mapper

QRadar Vulnerability Manager puede acceder al registro remoto a través de NetBIOS clásico (puertos 135, 137, 139) o del más reciente NetBIOS sobre TCP (en el puerto 445). Los cortafuegos de red o personales que bloquean el acceso a cualquiera de estos protocolos impiden el acceso las exploraciones de parches de Windows.

Las cuentas de usuarios administrativos tienen acceso al registro remoto de forma predeterminada. Las cuentas de usuarios no administrativos no tienen acceso al registro remoto. Debe configurar el acceso.

Habilitar el acceso remoto al Registro en el sistema operativo Windows

Para explorar sistemas Windows, debe configurar el Registro.

Procedimiento

1. Inicie una sesión en el sistema Windows.
2. Pulse **Inicio**.
3. En el campo **Buscar programas y archivos**, escriba **servicios** y pulse Intro.
4. En la ventana Servicios, localice el servicio **Registro remoto**.
5. Pulse con el botón derecho en el servicio **Registro remoto** y seleccione **Iniciar**.
6. Cierre la ventana Servicios.

Asignación de permisos de registro remoto mínimos

Las cuentas de usuarios administrativos tienen acceso al registro remoto de forma predeterminada. Las cuentas de usuarios no administrativos no tienen acceso al registro remoto. Debe configurar el acceso.

Procedimiento

1. En el sistema Windows de destino, cree o designe un usuario local o global (por ejemplo, "QVM_scan_user") y asigne acceso de registro de sólo lectura a la cuenta del usuario no administrativo.
2. Inicie la sesión en el sistema Windows mediante una cuenta que tenga privilegios de administrador. Pulse **Inicio** > **Ejecutar**.
3. Escriba `regedit`.
4. Pulse **Aceptar**.
5. Vaya a la clave:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers \winreg.

   Los permisos asociados a esta clave de registro controlan qué usuarios o qué grupo puede acceder de forma remota al registro desde la red.
6. Resalte la clave **winreg** y realice uno de los pasos siguientes:
   - En Windows XP o posterior, pulse **Editar** > **Permisos**.
   - En Windows 2000, pulse **Seguridad** > **Permisos**.
7. Otorgue acceso de solo lectura a la cuenta "QVM_scan_user" designada.

   En Windows XP, el valor *ForceGuest* está habilitado de forma predeterminada cuando se está en la modalidad de grupo de trabajo. Este valor puede provocar problemas de acceso para conexiones WMI y comparte acceso, otros servicios de DCOM y servicios de RPC. No puede inhabilitar el valor *ForceGuest* en sistemas Windows XP Home.

Configuración de Windows Management Instrumentation

QRadar Vulnerability Manager utiliza Windows Management Instrumentation (WMI) para buscar e identificar versiones de los archivos .exe y .dll instalados en los activos de destino que se exploran.

Acerca de esta tarea

Sin la información proporcionada por WMI, se pierden muchas aplicaciones de terceros. QRadar Vulnerability Manager no puede identificar ni eliminar los positivos falsos detectados durante la exploración del registro (mediante el servicio de registro remoto)

WMI está instalado en todos los sistemas operativos Windows modernos, como por ejemplo Windows Vista, Windows 2008, Windows 2012, Windows 7, Windows 8 y Windows 8.1).

El usuario de exploración debe habilitar las solicitudes de WMI remotas y debe hacerlas accesibles en los activos que se exploran. Si WMI no está disponible, se informa del error siguiente en los resultados de la exploración:

```
Error de comprobaciones locales - No se puede consultar el sistema de
archivos remoto serviceMount de WMI
```

En QRadar Vulnerability Manager versión 7.2.3 y posteriores, aparece un icono de aviso en forma de triángulo amarillo junto al activo, en los resultados de la exploración.

Si la exploración de parches no es satisfactoria, siga estos pasos.

Procedimiento

1. En el servidor de destino, vaya a **Panel de control** > **Herramientas administrativas** > **Gestión del sistema**.
2. Expanda **Servicios y aplicaciones**.
3. Pulse con el botón derecho del ratón sobre **Control de WMI** y pulse **Propiedades**.
4. Pulse la pestaña **Seguridad**.
5. Pulse **Seguridad**.
6. Opcional: Si es necesario, añada el usuario de supervisión y pulse el recuadro de selección **Habilitar remoto** para el usuario o el grupo que solicita datos de WMI. Para añadir un usuario o grupo de supervisión:
   a. Pulse **Añadir**.
   b. En el campo **Entrar nombres de objeto para seleccionar**, escriba el nombre del grupo o nombre de usuario.
   c. Pulse **Aceptar**.
7. Pulse **Avanzado** y aplique a los espacios de nombres root y sub.

   Nota: En algunos casos también deberá configurar los valores del cortafuegos de Windows y de DCOM.

   Si tiene problemas con WMI (Windows Management Interface), puede instalar las herramientas administrativas de WMI desde el sitio web de Microsoft.

   Las herramientas incluyen un navegador de WMI para conectar con una máquina remota y examinar la información de WMI. Estas herramientas le ayudan a identificar problemas de conectividad en un entorno más directo y sencillo.

Permitir solicitudes WMI a través del cortafuegos Windows

Para leer datos de WMI en un servidor remoto, se debe establecer una conexión entre el sistema de gestión (donde está instalado el software de supervisión) y el servidor que está supervisando. Si el servidor de destino está ejecutando el cortafuegos de Windows (también llamado Cortafuegos de conexión a Internet) que está instalado en sistemas Windows XP y Windows 2003, debe configurar el cortafuegos para permitir el paso de solicitudes de WMI remotas.

Para configurar el cortafuegos de Windows para permitir el paso de solicitudes de WMI remotas, abra un indicador de mandatos y especifique el mandato siguiente:

```
netsh firewall set service RemoteAdmin enable
```

Establecimiento de permisos de DCOM mínimos

Para conectar con un sistema remoto mediante WMI, debe asegurarse de que los valores de DCOM correctos y los valores de seguridad de espacio de nombres de WMI están habilitados para la conexión.

Acerca de esta tarea

Para otorgar permisos de activación e inicio remoto de DCOM para un usuario o un grupo, siga estos pasos.

Procedimiento

1. Pulse **Inicio** > **Ejecutar**, teclee `DCOMCNFG` y pulse **Aceptar**.
2. En el cuadro de diálogo **Servicios de componente**, expanda **Servicios de componente**, expanda **Sistemas** y pulse con el botón derecho del ratón sobre **Mi sistema** y pulse **Propiedades**.
3. En el cuadro de diálogo **Propiedades de mi sistema**, pulse la pestaña **Seguridad COM**.
4. En **Permisos de inicio y activación**, pulse **Editar límites**.
5. En el cuadro diálogo **Permiso de inicio**, si el nombre o el grupo no aparece en la lista **Nombres de grupos o usuarios**, siga estos pasos:
   a. En el cuadro de diálogo **Permiso de inicio**, pulse **Añadir**.
   b. En el cuadro de diálogo **Seleccionar usuarios, sistemas o grupos**, añada el nombre en el grupo en el cuadro **Entrar nombres de objeto para seleccionar** y pulse **Aceptar**.
6. En el cuadro de diálogo **Permiso de inicio**, seleccione el usuario y el grupo en el cuadro **Nombres de grupo o usuario**.
7. En la columna **Permitir**, bajo **Permisos para usuario**, seleccione **Inicio remoto**, seleccione **Activación remota** y a continuación pulse **Aceptar**.

Establecimiento de permisos de acceso remoto DCOM

Debe otorgar permisos de acceso remoto de DCOM a ciertos usuarios y grupos.

Acerca de esta tarea

Si el sistema A se conecta de forma remota con el sistema B, puede establecer estos permisos en el sistema B para permitir que un usuario o un grupo que no forme parte del grupo de administradores en el sistema B se conecte con el sistema B.

Procedimiento

1. Pulse **Inicio** > **Ejecutar**, teclee `DCOMCNFG` y pulse **Aceptar**.

2. En el cuadro de diálogo **Servicios de componente**, expanda **Servicios de componente**, expanda **Sistemas** y pulse con el botón derecho del ratón sobre **Mi sistema** y pulse **Propiedades**.
3. En el cuadro de diálogo **Propiedades de mi sistema**, pulse la pestaña **Seguridad COM**.
4. En **Permisos de acceso**, pulse **Editar límites**.
5. En el cuadro de diálogo **Permiso de acceso**, seleccione el nombre **ANONYMOUS LOGON** en el cuadro **Nombres de grupo o usuario**. En la columna **Permitir**, bajo **Permisos para usuario**, seleccione **Acceso remoto** y pulse **Aceptar**.

Recursos compartidos administrativos

Todos los sistemas Windows tienen recursos compartidos administrativos, `\\nombreMáquina\letraUnidad$` habilitados, especialmente cuando forman parte de un dominio.

QRadar Vulnerability Manager utiliza recursos compartidos administrativos para detectar vulnerabilidades en el conjunto limitado de aplicaciones siguiente:

- Mozilla Firefox
- Mozilla Thunderbird
- Java FX
- Apache Archiva
- Apache Continuum
- Google ChromePreferencias

Los comportamientos administrativos no son visibles para usuarios no administrativos y algunas organizaciones inhabilitan los recursos compartidos administrativos o utilizan cuentas de usuarios no administrativos para la exploración. Si no se puede acceder a los recursos compartidos no administrativos, es posible que QRadar Vulnerability Manager se pierda vulnerabilidades en los productos de la lista precedente o genere positivos falsos. En general, las pruebas de vulnerabilidad de QRadar Vulnerability Manager utilizan solo recursos compartidos administrativos como último recurso y utilizan exploraciones de registro y WMI.

Habilitación de recursos compartidos administrativos

En Windows Vista o versiones posteriores, los recursos compartidos administrativos están inhabilitados de forma predeterminada cuando se está en la modalidad “grupo de trabajo”.

Acerca de esta tarea

Habilite los recursos compartidos administrativos mediante estos pasos:

Procedimiento

1. Pulse **Inicio** > **Ejecutar** y escriba `regedit`.
2. Vaya a la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Pulse con el botón derecho del ratón sobre **Control de WMI** y pulse **Propiedades**.
4. Añada un DWORD llamado: `LocalAccountTokenFilterPolicy`
5. Establezca el valor en 1.

Inhabilitación de recursos compartidos administrativos

Algunas organizaciones no desean habilitar los recursos compartidos administrativos. Sin embargo, al habilitar el servicio de registro remoto, se inicia el servicio del servidor y los recursos compartidos administrativos están habilitados.

Acerca de esta tarea

Para inhabilitar los recursos compartidos administrativos, modifique la clave de registro siguiente:

Procedimiento

1. Pulse **Inicio** > **Ejecutar** y escriba `regedit`.
2. Vaya a la clave: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer**
3. Establezca el parámetro **`AutoShareWks`** en `0`.

   Nota: Esta acción no inhabilita el recurso compartido IPC$. Aunque este recurso compartido no se utiliza para acceder directamente a los archivos, asegúrese de que el acceso anónimo a este recurso compartido está inhabilitado. También puede eliminar completamente el recurso compartido IPC$ suprimiéndolo en el arranque utilizando el mandato siguiente:

   ```
   net share IPC$ /delete
   ```

   Utilice este método para eliminar también los recursos compartidos C$ y D$.

Configurar un intervalo de exploración permitida

En IBM Security QRadar Vulnerability Manager, puede crear un intervalo operativo para especificar el momento en que se puede ejecutar una exploración.

Acerca de esta tarea

Si una exploración no finaliza en el intervalo operativo, se pone en pausa y continúa cuando el intervalo operativo se vuelve a abrir. Para configurar un intervalo operativo:

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo** > **Intervalo operativo**.
3. En la barra de herramientas, pulse **Acciones** > **Añadir**.
4. Especifique un nombre para el intervalo operativo en el campo **Nombre**.
5. Lo sé
6. Elija una planificación de intervalo operativo en la lista **Planificación**.
7. Opcional: Seleccione los días en que se puede realizar la exploración.
8. Opcional: Seleccione su zona horaria.
9. Si ha seleccionado **Semanal** en la lista **Planificación**, marque los recuadros de selección de los días de la semana deseados en el área **Semanal**.
10. Si ha seleccionado **Mensualmente** en la lista **Planificación**, seleccione un día en la lista **Día del mes**.
11. Pulse **Guardar**.

Los intervalos operativos se pueden asociar con los perfiles de exploración mediante la pestaña **Cuándo explorar** de la página Configuración de perfil de exploración.

Si asigna dos ventanas operativas superpuestas a un perfil de exploración, el perfil de exploración se ejecuta desde el principio de la ventana operativa más antigua hasta el final de la ventana operativa más reciente. Por ejemplo, si configura dos intervalos operativos diarios para los periodos 01:00 a 06:00 y 05:00 a 09:00 horas, la exploración se ejecuta entre la 01:00 y las 09:00.

Para las ventanas operativas que no se solapan, la exploración empieza en la ventana operativa más antigua, se detiene si hay un intervalo entre las ventanas operativas y se reanuda al principio de la siguiente ventana operativa.

Explorar durante las horas permitidas

En IBM Security QRadar Vulnerability Manager, puede planificar una exploración de los activos de red para que se ejecute en horas permitidas, mediante el uso de un intervalo operativo.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Intervalo operativo**.
3. En la barra de herramientas, seleccione **Acciones** > **Añadir**.
4. Escriba un nombre para el intervalo operativo, configure un intervalo de tiempo permitido y pulse **Guardar**.
5. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
6. En la barra de herramientas, pulse **Añadir**.

   Cuando se crea un perfil de exploración, los únicos campos obligatorios son **Nombre** y **Direcciones IP** en la pestaña **Detalles** de la página Configuración del perfil de exploración. Para configurar la exploración durante las horas permitidas, también debe seguir los pasos restantes de este procedimiento.
7. Pulse la pestaña **Cuándo explorar**.
8. En la lista **Ejecutar planificación**, seleccione **Diariamente**.
9. En los campos **Hora de inicio**, escriba o seleccione la fecha y la hora en que desee que se ejecute la exploración cada día.
10. En el panel **Intervalos operativos**, seleccione un intervalo operativo en la lista y pulse (>).
11. Pulse **Guardar**.

Gestionar intervalos operativos

En IBM Security QRadar Vulnerability Manager, puede editar, suprimir y visualizar intervalos operativos.

Recuerde: Puede editar un intervalo operativo mientras está asociado a un perfil de exploración.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Intervalo operativo**.
3. Seleccione el intervalo operativo que desee editar.

4. En la barra de herramientas, seleccione una opción del menú **Acciones**.
5. Siga las instrucciones de la interfaz de usuario.

   Restricción: No puede suprimir un intervalo operativo que está asociado a un perfil de exploración. Debe primero desconectar el intervalo operativo respecto del perfil de exploración.

Desconectar un intervalo operativo

Si desea suprimir un intervalo operativo que está asociado a un perfil de exploración, debe desconectar el intervalo operativo respecto del perfil de exploración.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. Seleccione el perfil de exploración que desee editar.
4. En la barra de herramientas, pulse **Editar**.
5. Pulse el panel **Cuándo explorar**.
6. Seleccione la opción relevante de la lista **Ejecutar planificación** según convenga.
7. En el campo **Nombre**, seleccione el intervalo operativo que desea desconectar y pulse <.
8. Pulse **Guardar**.

Exploraciones de vulnerabilidades dinámicas

En IBM Security QRadar Vulnerability Manager, puede configurar una exploración para utilizar determinados exploradores de vulnerabilidades con rangos de CIDR determinados de la red. Por ejemplo, los exploradores pueden tener acceso solamente a determinadas áreas de la red.

Durante una exploración, QRadar Vulnerability Manager determina qué explorador debe utilizar para cada rango de CIDR, de dirección IP o de IP especificado en el perfil de exploración.

Exploración dinámica y dominios

Si ha configurado dominios en la ventana Gestión de dominios en la pestaña **Admin**, puede asociar exploradores con los dominios que ha añadido.

Por ejemplo, puede asociar cada explorador con un dominio diferente o con rangos de CIDR diferentes dentro del mismo dominio. QRadar explora dinámicamente los rangos de CIDR configurados que contienen las direcciones IP que especifique en todos los dominios que están asociadas con los exploradores del sistema. Los activos con la misma dirección IP en dominios distintos se exploran individualmente si el rango de CIDR para cada dominio incluye la dirección IP. Si una dirección IP no está dentro de un rango de CIDR configurado para un dominio de explorador, QRadar explora el dominio que está configurado para el explorador de controlador correspondiente al activo.

Configuración de una exploración dinámica

Para utilizar la *exploración dinámica*, siga estos pasos:

1. Añada exploradores de vulnerabilidades al despliegue de QRadar Vulnerability Manager. Para obtener más información, consulte "Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7.
2. Asocie exploradores de vulnerabilidades a rangos de CIDR y dominios.
3. Configure una exploración de varios rangos de CIDR y habilite **Selección dinámica de servidor** en la pestaña **Detalles** de la página Configuración de perfil de exploración.

Conceptos relacionados:

"Exploración dinámica" en la página 17
En la exploración dinámica, IBM Security QRadar Vulnerability Manager selecciona un explorador según la dirección IP que se explorará.

"Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7
Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

"Detalles de perfil de exploración" en la página 35
En IBM Security QRadar Vulnerability Manager puede describir una exploración, seleccionar el explorador que desea utilizar y elegir entre varias opciones de política de exploración.

Asociar exploraciones de vulnerabilidades a rangos de CIDR

En IBM Security QRadar Vulnerability Manager, para realizar una exploración dinámica, debe asociar exploradores de vulnerabilidades a segmentos diferentes de la red.

Antes de empezar

Debe añadir exploradores de vulnerabilidades adicionales al despliegue. Para obtener más información, consulte "Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Exploradores**.

   Atención: De forma predeterminada se muestra el explorador de controlador. El explorador de controlador forma parte del procesador de QRadar Vulnerability Manager que se despliega en la consola de QRadar o en un dispositivo de proceso dedicado de QRadar Vulnerability Manager. Puede asignar un rango de CIDR al explorador de controlador, pero debe desplegar exploradores adicionales para utilizar la exploración dinámica.
3. Seleccione un explorador en la página **Exploradores**.
4. En la barra de herramientas, pulse **Editar**.

   Restricción: No puede editar el nombre del explorador. Para editar un nombre de explorador, pulse **Admin** > **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
5. En el campo **CIDR**, escriba un rango de CIDR o varios rangos de CIDR separados por comas.

6. Pulse **Guardar**.

Conceptos relacionados:

"Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7
Si tiene una red grande y necesita opciones de exploración flexibles, puede añadir más exploradores al despliegue de IBM Security QRadar Vulnerability Manager.

Explorar rangos de CIDR con exploradores de vulnerabilidades diferentes

En IBM Security QRadar Vulnerability Manager, puede explorar áreas de una red con diferentes exploradores de vulnerabilidades.

Antes de empezar

Debe configurar los rangos de CIDR de red para utilizar los diferentes exploradores de vulnerabilidades en el despliegue de QRadar Vulnerability Manager. Para obtener más información, consulte "Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager" en la página 7.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir**.
4. Pulse la casilla **Selección de servidor dinámica**.

   Si ha configurado dominios en la ventana **Admin** > **Gestión de dominios**, puede seleccionar un dominio de la lista **Dominio**. Solamente se exploran los activos dentro del dominio seleccionado.
5. Opcional: Añada más rangos de CIDR.
6. Pulse **Guardar**.
7. Pulse el recuadro de selección en la fila que se ha asignado a la exploración en la página Perfiles de exploración y pulse **Ejecutar**.

Políticas de exploración

Una política de exploración proporciona una ubicación central para configurar los requisitos específicos de exploración.

Puede utilizar políticas de exploración para especificar los tipos de exploración, los puertos que deben explorarse, las vulnerabilidades que se explorarán y las herramientas de exploración que se usarán. En IBM Security QRadar Vulnerability Manager, un perfil de exploración tiene una *política de exploración* asociada que se utiliza para controlar una exploración de vulnerabilidades. Utilice la lista **Políticas de exploración** de la pestaña **Detalles** de la página Configuración del perfil de exploración para asociar una política de exploración con un perfil de exploración.

Puede crear una nueva política de exploración, o copiar y modificar una política preconfigurada que se distribuye con QRadar Vulnerability Manager.

Políticas de exploración preconfiguradas

Las políticas de exploración preconfiguradas siguientes se distribuyen con QRadar Vulnerability Manager:

- Exploración completa
- Exploración de descubrimiento
- Exploración de bases de datos
- Exploración de parches
- Exploración de PCI
- Exploración de web

La página Políticas de exploración muestra una descripción de cada política de exploración preconfigurada.

Tareas relacionadas:

"Modificar una política de exploración preconfigurada"
En IBM Security QRadar Vulnerability Manager, puede copiar una política de exploración preconfigurada y modificarla de acuerdo con sus necesidades específicas de exploración.

"Configurar una política de exploración para gestionar las exploraciones de vulnerabilidades" en la página 62
En IBM Security QRadar Vulnerability Manager, puede configurar una política de exploración para controlar las exploraciones de vulnerabilidades.

Actualizaciones automáticas de política de exploración para vulnerabilidades críticas

Como parte de las actualizaciones automáticas diarias de IBM Security QRadar Vulnerability Manager, se reciben nuevas políticas de exploración para tareas tales como detectar vulnerabilidades de ataque de día-cero en los activos.

Utilice las políticas de exploración suministradas por la actualización automática para crear perfiles de exploración destinados a explorar vulnerabilidades específicas. Para ver todas las políticas de exploración del sistema, vaya a **Administrativo** > **Políticas de exploración** en la pestaña **Vulnerabilidades**.

No debe editar políticas de exploración suministradas por la actualización automática, ya que actualizaciones posteriores podrían sobrescribir los cambios. Puede crear una copia y editarla.

Si suprime una política de exploración suministrada por la actualización automática, sólo podrá recuperarla mediante el soporte al cliente de QRadar.

Modificar una política de exploración preconfigurada

En IBM Security QRadar Vulnerability Manager, puede copiar una política de exploración preconfigurada y modificarla de acuerdo con sus necesidades específicas de exploración.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Políticas de exploración**.
3. En la página Políticas de exploración, pulse una política de exploración preconfigurada.
4. En la barra de herramientas, pulse **Editar**.
5. Pulse **Copiar**.

6. En la ventana Copiar política de exploración, escriba un nombre nuevo en el campo **Nombre** y pulse **Aceptar**.
7. Pulse en la copia de la política de exploración y seleccione **Editar** en la barra de herramientas.
8. En el campo **Descripción**, escriba nueva información sobre la política de exploración.

   Importante: Si modifica la política de exploración nueva, debe actualizar la información contenida en la descripción.
9. Para modificar la política de exploración, utilice las pestañas **Exploración de puertos**, **Vulnerabilidades**, **Grupos de herramientas** o **Herramientas**.

   Restricción: Dependiendo del valor que seleccione en **Tipo de exploración**, no puede utilizar todas las pestañas de la ventana Política de exploración.

Configurar una política de exploración para gestionar las exploraciones de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede configurar una política de exploración para controlar las exploraciones de vulnerabilidades.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Administrativo** > **Políticas de exploración**.
3. En la barra de herramientas, pulse **Añadir**.
4. Escriba el nombre y la descripción de la política de exploración.

   Para configurar una política de exploración, los únicos campos obligatorios de la ventana Política de exploración nueva son los campos **Nombre** y **Descripción**.
5. En la lista **Tipo de exploración**, seleccione el tipo de exploración en la que basar la política de exploración.
6. Para incluir vulnerabilidades determinadas en la política de exploración, realice los pasos siguientes:
   a. En la ventana Política de exploración nueva, marque el recuadro de selección **Parche**.
   b. Pulse la pestaña **Vulnerabilidades**.
   c. Pulse **Añadir**.

      De forma predeterminada se muestran todas las vulnerabilidades descubiertas durante el último año.
   d. Filtre la lista de vulnerabilidades.
   e. Seleccione las vulnerabilidades que desee incluir en la política de exploración y pulse **Someter** en la barra de herramientas.
7. Para incluir o excluir grupos de herramientas de una política sin credenciales o de exploración completa, pulse la pestaña **Grupo de herramientas**.
8. Para incluir o excluir herramientas de una política sin credenciales o de exploración completa, pulse la pestaña **Herramientas**.

   Importante:

Si no modifica las herramientas o grupos de herramientas y ha seleccionado la opción **Completa**, todas las herramientas y grupos de herramientas que están asociados a una exploración completa se incluyen en la política de exploración.

9. Pulse **Guardar**.

Capítulo 6. Investigación de exploraciones de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede investigar datos de resumen de activo y de vulnerabilidad para cada exploración.

Para investigar exploraciones de vulnerabilidades, puede realizar las tareas siguientes:

- Crear y guardar criterios de búsqueda complejos para vulnerabilidades.
- Investigar niveles de riesgo de explotación para cada red, activo y vulnerabilidad.
- Priorizar los procesos de corrección de vulnerabilidades.

Resultados de exploración

Puede utilizar la página Resultados de exploración para investigar la información siguiente:

- El progreso de una exploración y las herramientas de exploración que están en cola y en ejecución.
- El estado de una exploración. Por ejemplo, una exploración cuyo estado es **Detenido** indica que la exploración ha finalizado satisfactoriamente o se ha cancelado.
- El grado de riesgo que está asociado a cada perfil de exploración completado. El riesgo se indica mediante la columna **Puntuación** y muestra la puntuación CVSS (Common Vulnerability Scoring System) del perfil de exploración completado.
- El número total de activos que fueron encontrados por la exploración.
- El número total de vulnerabilidades que fueron encontradas por el perfil de exploración completado.
- El número total de servicios abiertos fueron descubiertos por el perfil de exploración completado.

Recuentos de vulnerabilidades

La página Resultados de exploración muestra **Vulnerabilidades** e **Instancias de vulnerabilidad**.

- La columna **Vulnerabilidades** muestra el número total de vulnerabilidades exclusivas que se descubrieron en todos los activos explorados.
- Cuando explora varios activos, una misma vulnerabilidad puede estar presente en activos diferentes. Por lo tanto, la columna **Instancias de vulnerabilidad** muestra el número total de vulnerabilidades que se descubrieron en todos los activos explorados.

Buscar resultados de exploración

En IBM Security QRadar Vulnerability Manager, puede buscar y filtrar resultados de exploración.

Por ejemplo, puede identificar exploraciones recientes, exploraciones para una dirección IP determinada o exploraciones que identificaron una vulnerabilidad determinada.

Acerca de esta tarea

Utilice el campo **Nombre** en la pestaña **Vulnerabilidades** para buscar en los resultados por nombre de perfil de exploración. Para utilizar criterios más avanzados en la búsqueda, haga lo siguiente:

Las restricciones de nivel de dominio no se aplican hasta que los perfiles de seguridad se han actualizado con un dominio asociado y se han desplegado los cambios.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Resultados de exploración**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.

   Para buscar resultados de exploración, no existen campos obligatorios. Todos los parámetros son opcionales.
4. Para mostrar los resultados de las exploraciones que se han completado dentro de un número reciente de días, escriba un valor en el campo **Exploración ejecutada en los últimos días**.
5. Para mostrar los resultados de exploración para una vulnerabilidad determinada, pulse **Examinar** en el campo **Contiene vulnerabilidad**.
6. Para mostrar los resultados de las exploraciones que sólo se han planificado, pulse **Excluir exploración bajo demanda**.
7. Pulse **Buscar**.

Conceptos relacionados:

"Planificación de exploración" en la página 37
En IBM Security QRadar Vulnerability Manager, puede planificar las fechas y horas en que es conveniente explorar los activos de red para buscar vulnerabilidades conocidas.

Incluir cabeceras de columna en las búsquedas de activos

Puede limitar las búsquedas de activos con filtros que incluyen perfiles de activo personalizados, nombre, recuento de vulnerabilidades y puntuación de riesgo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activos**, y en la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
3. En el campo del lado izquierdo que contiene nombres de columna, pulse las cabeceras de columna que desee incluir en la búsqueda y pulse el botón de flecha para trasladar las cabeceras seleccionadas al campo situado en el lado derecho.
4. Pulse los botones de flecha arriba y flecha abajo para cambiar la prioridad de las cabeceras de columna seleccionadas.
5. Cuando el campo del lado derecho contenga todas las cabeceras de columna para las que desee buscar, pulse **Buscar**.

Gestionar resultados de exploración

En la página Resultados de exploración de IBM Security QRadar Vulnerability Manager, puede gestionar los resultados de exploración y las exploraciones que están en ejecución.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Resultados de exploración**.
3. Opcional: Si desea volver a ejecutar exploraciones completadas, marque el recuadro de selección en las filas asignadas a las exploraciones y pulse **Ejecutar**.

   El estado de una exploración completada es **Detenido**.
4. Opcional: Para suprimir resultados de exploración completada:
   a. En la página Resultados de la exploración, marque el recuadro de selección de las filas asignadas a los resultados de búsqueda que desea suprimir.
   b. En la barra de herramientas, pulse **Suprimir**.

      Si suprime un conjunto de resultados de exploración, no se visualiza ningún aviso. Los resultados de exploración se suprimen inmediatamente.

      Recuerde: Cuando suprime un conjunto de resultados de exploración, no se suprimen los datos de exploración del modelo de activos de QRadar ni del perfil de exploración.
5. Opcional: Para cancelar una exploración que está en ejecución:
   a. En la página Resultados de la exploración, marque el recuadro de selección de las filas asignadas a las exploraciones que desea cancelar.
   b. En la barra de herramientas, pulse **Cancelar**.

      Puede cancelar una exploración cuyo estado sea **En ejecución** o **En pausa**. Después de cancelar una exploración, el estado de la exploración es **Detenido**.

Niveles de riesgo de activos y categorías de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, utilice la página Resultados de exploración (Activos) para investigar el nivel de riesgo de explotación de los activos explorados.

La página Resultados de exploración (Activos) proporciona un resumen de riesgos y vulnerabilidades para cada activo que se ha explorado mediante la ejecución de un perfil de exploración.

Puntuación de riesgo

Cada vulnerabilidad que se ha detectado en la red tiene una puntuación de riesgo que se calcula mediante la puntuación base de CVSS (Common Vulnerability Scoring System). Una puntuación de riesgo alta proporciona una indicación de la posibilidad de una explotación de vulnerabilidad.

La columna **Puntuación** de la página Resultados de exploración (Activos) es una puntuación de riesgo acumulada para cada vulnerabilidad detectada en un activo. Este valor acumulado proporciona una indicación del nivel de riesgo que está asociado a cada activo.

Para identificar rápidamente los activos que tiene un mayor riesgo de explotación de vulnerabilidad, pulse la cabecera de la columna **Puntuación** para ordenar los activos de acuerdo con el nivel de riesgo.

Recuentos y categorías de vulnerabilidades

La página Resultados de exploración (Activos) muestra el número total de vulnerabilidades y servicios abiertos que se han descubierto en cada activo explorado.

Para identificar los activos con el mayor número de vulnerabilidades, pulse la cabecera de la columna **Instancias de vulnerabilidad** para ordenar los activos.

Las columnas **Alto**, **Medio**, **Bajo** y **Aviso** agrupan todas las vulnerabilidades de acuerdo con su riesgo.

Las columnas **% de comprobaciones de políticas aprobadas** y **% de comprobaciones de política fallidas** muestran el porcentaje de comprobaciones de política que el activo ha pasado o no ha pasado en la exploración de referencia. Pulse los valores de estas columnas para ver más información sobre las comprobaciones de política que han pasado o que no han pasado en la página Resultados de exploración (Comprobaciones de política).

Datos de activo, de vulnerabilidad y de servicios abiertos

En IBM Security QRadar Vulnerability Manager, la página Resultados de exploración (Detalles de activo) muestra datos de activo, de vulnerabilidad y de servicios abiertos.

Mediante las opciones de la barra de herramientas, puede conmutar entre ver vulnerabilidades y servicios abiertos.

La página Resultados de exploración (Detalles de activo) proporciona la información siguiente:

- Información de resumen sobre el activo que se exploró, incluido el sistema operativo y grupo de red.
- Una lista de las vulnerabilidades o servicios abiertos que se han descubierto en el activo explorado.
- Diversas formas de clasificar y ordenar la lista de vulnerabilidades o servicios abiertos, por ejemplo, por **Riesgo**, **Gravedad** y **Puntuación**.
- Una manera rápida de ver información sobre servicios abiertos o vulnerabilidades. En la barra de herramientas, pulse **Vulnerabilidades** o **Servicios abiertos**.
- Una manera fácil de ver información detallada sobre el activo que se exploró. En la barra de herramientas, pulse **Detalles de activo**.
- Un método alternativo de crear una excepción de vulnerabilidad. En la barra de herramientas, pulse **Acciones** > **Excepción**.

El icono de precaución indica que la exploración ha fallado. Pase el cursor del ratón sobre el icono para obtener detalles adicionales.

Para obtener más información sobre la ventana Detalles de activo, consulte la *Guía del usuario* del producto.

Conceptos relacionados:

Capítulo 8, “Reglas de excepción de vulnerabilidad”, en la página 87
En IBM Security QRadar Vulnerability Manager, puede configurar reglas de excepción para reducir el número de vulnerabilidades de falso positivo.

Ver el estado de descarga de parches de activos

Ver si un activo tiene una descarga de parches pendiente. Si no hay ninguna descarga pendiente, el activo tiene todos los parches disponibles.

Procedimiento

1. Busque el activo para el que desee verificar el estado de descarga de parches.
2. Pulse la Dirección IP de activo para abrir la ventana **Detalles de activo**.
3. Pulse **Detalles** > **Propiedades** para abrir la ventana **Propiedades de activo**.
4. Pulse la flecha **Parches de Windows**.
5. Vea el estado de parche en la columna **Pendiente**.
   - True: este valor indica que el activo tiene parches pendientes para descargar.
   - False: este valor indica que el activo no tiene descargas de parche pendientes.

Riesgo de vulnerabilidad y gravedad de PCI

En IBM Security QRadar Vulnerability Manager, puede revisar el riesgo y la gravedad de PCI (industria de las tarjetas de pago) para cada vulnerabilidad encontrada por una exploración.

Puede revisar la información siguiente:

- El nivel de riesgo que está asociado a cada vulnerabilidad.
- El número de activos de la red en los que se ha encontrado la vulnerabilidad específica.

Para investigar una vulnerabilidad, puede pulsar un enlace de vulnerabilidad en la columna **Vulnerabilidad**.

Notificar por correo electrónico el inicio y detención de las exploraciones de vulnerabilidades a los propietarios de activos

Notifique la planificación de exploraciones por correo electrónico a los propietarios de activos. También puede enviar informes por correo electrónico a los propietarios de activos.

Antes de empezar

Configure el servidor de correo del sistema y propietarios técnicos para activos. Para obtener más información, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. Pulse **Administrativo** > **Perfiles de exploración**.
3. En la fila asignada a la exploración que desee editar, marque el recuadro de selección y pulse **Editar** en la barra de herramientas.
4. En el área **¿Qué enviar por correo electrónico?** de la pestaña **Correo electrónico**, marque los recuadros de selección correspondientes.

5. Si ha marcado el recuadro de selección **Informes**, en el campo **Informes disponibles** seleccione los informes que desee enviar por correo electrónico y pulse la flecha para trasladar informes al campo **Informes seleccionados**.

   Los informes pueden ser grandes. Compruebe que los informes enviados no son rechazados por el proveedor de correo electrónico del destinatario.
6. En el área **¿A quién enviar correo electrónico?**, seleccione los destinatarios que desee que reciban los correos electrónicos:
   - Para enviar correo electrónico a los propietarios técnicos configurados de los activos explorados, seleccione la casilla **Propietarios técnicos**. Los propietarios técnicos recibirán correos electrónicos referentes a sus activos solamente.
   - Para escribir o seleccionar direcciones de correo electrónico en el campo, seleccione la casilla **Direcciones de destino**. Seleccione direcciones de correo electrónico y pulse **Añadirme** para enviar correo electrónico a los destinatarios de correo electrónico seleccionados. Las direcciones de correo electrónico especificadas recibirán correos electrónicos e informes referentes a todos los activos explorados.
7. Pulse **Guardar**.

Capítulo 7. Gestión de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede gestionar, buscar y filtrar datos de vulnerabilidad para centrar su atención en las vulnerabilidades que representan el mayor riesgo para su empresa.

Los datos de vulnerabilidad que se muestran están basados en la información de estado de vulnerabilidad que se mantiene en el modelo de activos de QRadar. Esta información incluye las vulnerabilidades encontradas por el explorador de QRadar Vulnerability Manager y las vulnerabilidades importadas desde productos de exploración externos.

Gestione las vulnerabilidades para proporcionar la información siguiente:

- Una vista de red de su situación actual respecto a las vulnerabilidades.
- Identifique las vulnerabilidades que representan el riesgo mayor para su empresa y asigne vulnerabilidades a usuarios de QRadar para su corrección.
- Determine en qué grado las vulnerabilidades afectan a la red y visualice información detallada sobre los activos de red que contienen vulnerabilidades.
- Determine qué vulnerabilidades representan menos riesgo para su empresa y cree excepciones de vulnerabilidad.
- Visualice información histórica sobre las vulnerabilidades de la red.
- Visualice datos de vulnerabilidad para cada red, activo, servicio abierto o instancia de vulnerabilidad.

Investigar puntuaciones de riesgo de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede investigar puntuaciones de riesgo de vulnerabilidades y conocer cómo se calcula cada puntuación.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. Opcional: Pulse la columna **Puntuación de riesgo** para ordenar las vulnerabilidades de acuerdo con el riesgo.
4. Para investigar la puntuación de riesgo, pase el puntero del ratón sobre una puntuación de riesgo de vulnerabilidad.

Detalles de puntuación de riesgo

En IBM Security QRadar Vulnerability Manager, las puntuaciones de riesgo de vulnerabilidad proporcionan una indicación del riesgo que una vulnerabilidad representa para su empresa.

Mediante IBM Security QRadar Risk Manager, puede configurar políticas que ajustan las puntuaciones de riesgo de vulnerabilidad y centran la atención en tareas de corrección importantes.

Puntuación de riesgo

La **puntuación de riesgo** proporciona contexto de red específico utilizando mediciones base de CVSS (Common Vulnerability Scoring System), temporales y del entorno.

Cuando QRadar Risk Manager se utiliza sin licencia, la columna **Puntuación de riesgo** muestra la puntuación de métrica de entorno CVSS con un valor máximo de 10.

Subpuntuación de explotabilidad

La explotabilidad se calcula como subconjunto de la puntuación base de CVSS utilizando los elementos siguientes:

- El Vector de acceso proporciona una indicación de riesgo que está basada en el grado de lejanía de un atacante, tal como red local o adyacente.
- La Complejidad de acceso proporciona una indicación de riesgo que está basada en la complejidad del ataque. Cuanto menor es la complejidad, mayor es el riesgo.
- La Autenticación proporciona una indicación de riesgo que está basada en los intentos de autenticación. Cuanto menor es el número de intentos, mayor es el riesgo.

Ajustes de riesgo

Si IBM Security QRadar Risk Manager está instalado y ha configurado políticas de riesgo de vulnerabilidad, aparecen listados los ajustes de riesgo. Los ajustes aumentan o reducen el riesgo global que está asociado a una vulnerabilidad.

Conceptos relacionados:

"Integración de QRadar Risk Manager y QRadar Vulnerability Manager" en la página 23
IBM Security QRadar Vulnerability Manager se integra con IBM Security QRadar Risk Manager para ayudarle a priorizar riesgos y vulnerabilidades en la red.

Tareas relacionadas:

"Priorizar vulnerabilidades de alto riesgo mediante la aplicación de políticas de riesgo" en la página 81
En IBM Security QRadar Vulnerability Manager, puede alertar a los administradores respecto a las vulnerabilidades de alto riesgo aplicando políticas de riesgo a las vulnerabilidades.

Buscar datos de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

QRadar Vulnerability Manager proporciona varios métodos para buscar datos. Puede buscar por red, por activo, por servicio abierto o por vulnerabilidad.

Las búsquedas guardadas predeterminadas proporcionan un forma rápida de identificar riesgos para la empresa. Las búsquedas guardadas se visualizan en el campo **Búsquedas guardadas disponibles** de la página Búsqueda del gestor de vulnerabilidades.

Antes de empezar

Debe crear un perfil de exploración y explorar los activos de la red.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. Si desea cargar una búsqueda guardada, realice los pasos siguientes:
   a. Opcional: Seleccione un grupo en la lista **Grupo**.
   b. Opcional: En el campo **Escribir búsqueda guardada**, escriba la búsqueda guardada que desee cargar.
   c. En la lista **Búsquedas guardadas disponibles**, seleccione una búsqueda guardada y pulse **Cargar**.
   d. Pulse **Buscar**.
5. Si desea crear una búsqueda nueva, siga los pasos siguientes en el panel Parámetros de búsqueda:
   a. En la **primera lista**, seleccione el parámetro que desee utilizar.
   b. En la **segunda lista**, seleccione un modificador de búsqueda. Los modificadores que están disponibles dependen del parámetro de búsqueda que seleccione.
   c. En la **tercera lista**, escriba o seleccione la información específica que está relacionada con el parámetro de búsqueda.
   d. Pulse **Añadir filtro**.

   Por ejemplo, para enviar por correo electrónico las vulnerabilidades que están asignadas a un usuario técnico, seleccione **Contacto de propietario técnico** y proporcione una dirección de correo electrónico que esté configurada en la página Asignación de vulnerabilidades.
6. Pulse **Buscar**.
7. Opcional: En la barra de herramientas, pulse **Guardar criterios de búsqueda**.

   Importante: Los informes de vulnerabilidad utilizan información de búsquedas guardadas. Si desea crear un informe que envía un correo electrónico a un usuario técnico, debe guardar los criterios de búsqueda.

Conceptos relacionados:

"Parámetros de búsqueda de vulnerabilidades" en la página 74
En IBM Security QRadar Vulnerability Manager, puede buscar datos de vulnerabilidad y guardar las búsquedas para un uso futuro.

Búsquedas rápidas de vulnerabilidades

Busque las vulnerabilidades escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

En IBM Security QRadar Vulnerability Manager puede utilizar búsquedas rápidas para filtrar las vulnerabilidades en las páginas Mis vulnerabilidades asignadas y Gestionar vulnerabilidades.

Utilice la lista **Búsquedas rápidas** para realizar una búsqueda de vulnerabilidades preconfigurada.

Utilice el campo **Filtro rápido** para crear sus propios filtros de vulnerabilidades. Pulse **Guardar criterios de búsqueda** para añadir filtros rápidos de vulnerabilidades a la lista **Búsquedas rápidas**.

Tabla 5. Directrices de sintaxis del filtro rápido de vulnerabilidades

Descripción	Ejemplo

Incluir un texto sin formato que espere encontrar en el título, la descripción, la solución, la preocupación, el tipo de ID de referencia o el valor de ID de referencia de la vulnerabilidad.	`2012-3764`
	
	`MS203`
	
	`java`

Para buscar el texto solamente en el título de la vulnerabilidad, añadir **A:** a la serie de texto de búsqueda	`PHP:A`
Para buscar el texto solamente en la descripción de la vulnerabilidad, añadir **B:** a la serie de texto de búsqueda	`cross-site scripting:B`
Para buscar el texto solamente en el tipo de referencia externa de la vulnerabilidad, añadir **C:** a la serie de texto de búsqueda	`RedHat RHSA:C`
Incluir caracteres comodín. El término de búsqueda no puede empezar por un comodín.	`SSLv*`

Agrupar términos con operadores lógicos: **AND**, **OR** y **NOT** (o **!**). Para que se reconozcan como operadores lógicos y no como términos de búsqueda, los operadores deben estar en mayúsculas.	`PHP AND Traversal`
	
	`XSS:A OR cross-site scripting:A`
	
	`!MySQL`
	
	`NOT MySQL`

Tareas relacionadas:

"Guardar criterios de búsqueda de vulnerabilidades" en la página 77
En IBM Security QRadar Vulnerability Manager, puede guardar criterios de búsqueda de vulnerabilidades para su uso en el futuro.

Parámetros de búsqueda de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede buscar datos de vulnerabilidad y guardar las búsquedas para un uso futuro.

La tabla siguiente no es una lista completa de parámetros de búsqueda de vulnerabilidades, sino un subconjunto de las opciones disponibles.

Seleccione cualquiera de los parámetros para buscar y visualizar datos de vulnerabilidad.

Tabla 6. Parámetros de búsqueda de vulnerabilidades

Opción	Descripción
Complejidad del acceso	Complejidad del ataque que es necesaria para explotar una vulnerabilidad.
Vector de acceso	Ubicación de red desde donde se puede explotar una vulnerabilidad.

Tabla 6. Parámetros de búsqueda de vulnerabilidades (continuación)

Opción	Descripción
Búsqueda guardada de activo	Host, dirección IP o rango de direcciones IP asociados a una búsqueda de activos guardada. Para obtener más información sobre cómo guardar búsquedas de activos, consulte la *Guía del usuario* del producto.
Activos con servicio abierto	Activos que tienen servicios abiertos determinados. Por ejemplo, HTTP, FTP y SMTP.
Autenticación	Número de veces que un atacante se debe autenticar con un destino para explotar una vulnerabilidad.
Efecto en la disponibilidad	Grado en que se puede poner en peligro la disponibilidad de recursos si se explota una vulnerabilidad.
Efecto en la confidencialidad	Nivel de información confidencial que se puede obtener si se explota una vulnerabilidad.
Días desde que se encontró el activo	Número de días transcurridos desde que el activo con la vulnerabilidad se descubrió en la red. Los activos se pueden descubrir mediante una exploración activa o de forma pasiva mediante análisis de archivos de registro o de flujos.
Días desde que se detectó tráfico de servicio de vulnerabilidad asociado	Muestra vulnerabilidades en activos con tráfico de la capa 7 intercambiado con un activo, de acuerdo con el número de días transcurridos desde que se detectó el tráfico.
Dominio	Si ha configurado IBM Security QRadar para sistemas de varios dominios, utilice esta opción para especificar el dominio en el que desea buscar vulnerabilidades.
Por servicio abierto	Utilice este parámetro para buscar vulnerabilidades que están asociadas con servicios abiertos determinados como HTTP, FTP y SMTP.
Referencia externa de tipo	Vulnerabilidades que tienen un Fixlet de IBM BigFix asociado. Mediante este parámetro puede hacer que se muestren solamente las vulnerabilidades sin un parche disponible.
Efecto	Efecto posible en la empresa. Por ejemplo, pérdida del control de accesos, tiempo de inactividad y pérdida de reputación.
Incluir avisos tempranos	Vulnerabilidades recién publicadas que se detectan en la red sin exploraciones adicionales.
Incluir excepciones de vulnerabilidad	Vulnerabilidades que tienen una regla de excepción aplicada a ellas.

Tabla 6. Parámetros de búsqueda de vulnerabilidades (continuación)

Opción	Descripción
Efecto en la integridad	Grado en que se puede poner en peligro la integridad del sistema si se explota una vulnerabilidad.
Incluir sólo activos con riesgo	Vulnerabilidades que cumplen o no políticas de riesgo determinadas que se definen y supervisan en IBM Security QRadar Risk Manager. **Nota:** Debe supervisar al menos una pregunta en la página Supervisor de políticas en la pestaña **Riesgos** para utilizar este parámetro de búsqueda.
Incluir solo activos con riesgo pasado	Vulnerabilidades que cumplen políticas de riesgo determinadas que se definen y supervisan en QRadar Risk Manager.
Incluir solo avisos tempranos	Utilice este parámetro para incluir solamente las vulnerabilidades recién publicadas que se detectan en la red sin exploraciones adicionales en la búsqueda.
Incluir solo excepciones de vulnerabilidad	Utilice este parámetro para incluir solamente las vulnerabilidades que tienen aplicada una regla de excepción en la búsqueda.
Vencido por días	Utilice este parámetro para buscar vulnerabilidades que están pendientes de corrección y que han vencido hace un número especificado de días.
Estado de parche	Utilice este parámetro para filtrar las vulnerabilidades por estado de parche. Para obtener más información, consulte “Identificar el estado de parche de las vulnerabilidades” en la página 83.
Gravedad de PCI	Utilice este parámetro para buscar vulnerabilidades por nivel de gravedad de PCI (alto, medio o bajo) asignado por el servicio de conformidad de PCI. Las vulnerabilidades asignadas a un nivel de gravedad alta o media de PCI no cumplen la conformidad de PCI.
Búsqueda rápida	Puede buscar de acuerdo con el nombre, descripción, solución o identificador de referencia externa de una vulnerabilidad. En el campo **Búsqueda rápida** puede utilizar los operadores AND, OR y NOT, así como corchetes.
Riesgo	Utilice este parámetro para buscar vulnerabilidades por nivel de riesgo (alto, medio, bajo, aviso).
Sin asignar	Utilice este parámetro para buscar vulnerabilidades sin usuario asignado para que las solucione.

Tabla 6. Parámetros de búsqueda de vulnerabilidades (continuación)

Opción	Descripción
Referencia externa de vulnerabilidad	Vulnerabilidades que están basadas en una lista importada de identificadores de vulnerabilidades, por ejemplo CVE ID. Para obtener más información sobre Conjuntos de referencia, consulte la *Guía de administración* del producto.
Vulnerabilidad con parche virtual del proveedor	Vulnerabilidades a las que se pueden aplicar parches mediante un sistema de prevención de intrusiones.
Estado de vulnerabilidad	El estado de la vulnerabilidad desde la última exploración de la red o de activos de red determinados. Por ejemplo, cuando explora activos, una vulnerabilidad descubierta pueden ser Nueva, Preexistente, Fija o Existente.
Vulnerabilidades con riesgo	Utilice este parámetro para filtrar las vulnerabilidades por resultados de política de riesgo. Debe supervisar al menos una pregunta en la página Supervisor de políticas en la pestaña **Riesgos** para utilizar este parámetro de búsqueda.

Guardar criterios de búsqueda de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede guardar criterios de búsqueda de vulnerabilidades para su uso en el futuro.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva** y realice la búsqueda de datos.
4. En la barra de herramientas, pulse **Guardar criterios de búsqueda**.
5. En la ventana Guardar criterios de búsqueda, escriba un nombre reconocible para la búsqueda guardada.
6. Opcional: Para incluir la búsqueda guardada en la lista **Búsquedas rápidas** de la barra de herramientas, pulse **Incluir en Búsquedas rápidas**.
7. Opcional: Para compartir los criterios de búsqueda guardados con todos los usuarios de QRadar, pulse **Compartir con todos**.
8. Opcional: Para colocar la búsqueda guardada en un grupo, pulse en un grupo o pulse **Gestionar grupos** para crear un grupo nuevo.

   Para obtener más información sobre la gestión de grupos de búsqueda, consulte la *Guía de administración* del producto.
9. Opcional: Si desea mostrar los resultados de la búsqueda guardada cuando pulsa cualquiera de las páginas Gestionar vulnerabilidades del panel de navegación, pulse **Establecer como predeterminado**.
10. Pulse **Aceptar**.

Suprimir criterios de búsqueda de vulnerabilidades guardados

En IBM Security QRadar Vulnerability Manager, puede suprimir criterios de búsqueda de vulnerabilidades guardados.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Gestionar vulnerabilidades** > **Por red**
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. En la lista **Búsquedas guardadas disponibles** de la página Búsqueda del gestor de vulnerabilidades, seleccione la búsqueda guardada que desee suprimir.
5. Pulse **Suprimir**.
6. Pulse **Aceptar**.

Instancias de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede visualizar las vulnerabilidades de cada activo explorado de la red. Cada vulnerabilidad puede aparecer listada varias veces si existe en varios activos.

Si configura exploradores externos de evaluación de vulnerabilidades mediante la pestaña QRadar **Admin**, las vulnerabilidades detectadas se muestran automáticamente en la página Por instancias de vulnerabilidad.

Para obtener más información sobre exploradores de evaluación de vulnerabilidades, consulte la *Guía de administración* del producto.

La página Por instancias de vulnerabilidad proporciona la información siguiente:

- Una vista de cada vulnerabilidad que se detectó al explorar activos de la red.
- Riesgo que cada vulnerabilidad representa para el sector de las tarjetas de pago (PCI).
- Riesgo que cada vulnerabilidad representa para su empresa. Pulse la columna **Puntuación de riesgo** para identificar las vulnerabilidades con el riesgo más alto.
- Nombre o dirección de correo electrónico del usuario que está asignado para corregir la vulnerabilidad.
- Número de días dentro de los cuales se debe corregir una vulnerabilidad.

Conceptos relacionados:

"Detalles de puntuación de riesgo" en la página 71
En IBM Security QRadar Vulnerability Manager, las puntuaciones de riesgo de vulnerabilidad proporcionan una indicación del riesgo que una vulnerabilidad representa para su empresa.

Vulnerabilidades de red

En IBM Security QRadar Vulnerability Manager, puede examinar datos de vulnerabilidad que están agrupados de acuerdo con la red.

La página Por red proporciona la información siguiente:

- Una puntuación de riesgo acumulada que está basada en las vulnerabilidades detectadas en cada red.
- Número de activos, vulnerabilidades y servicios abiertos de cada red.

- Número de vulnerabilidades que están asignadas a un usuario técnico y que están pendientes de corrección.

Vulnerabilidades de activos

En IBM Security QRadar Vulnerability Manager, puede visualizar datos de vulnerabilidad de resumen que están agrupados para cada activo explorado.

Puede utilizar la página Por activo para priorizar las tareas de corrección para activos de la empresa que están expuestos al riesgo mayor.

La página Por activo proporciona la información siguiente:

- Una puntuación de riesgo acumulada que está basada en las vulnerabilidades detectadas en cada activo.

  Pulse la columna **Puntuación de riesgo** para ordenar los activos de acuerdo con el riesgo al que están expuestos.
- Número de vulnerabilidades de activo que están asignadas a un usuario técnico y que están pendientes de corrección.

Vulnerabilidades de servicio abierto

En IBM Security QRadar Vulnerability Manager, puede visualizar datos de vulnerabilidad que están agrupados de acuerdo con el servicio abierto.

La página Por servicio abierto muestra una puntuación de riesgo acumulado y un recuento de vulnerabilidades para cada servicio de la red.

Investigar el historial de una vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede visualizar información útil sobre el historial de una vulnerabilidad.

Por ejemplo, puede obtener información sobre cómo se ha calculado la puntuación de riesgo de una vulnerabilidad. También puede revisar información sobre cuándo se descubrió una vulnerabilidad por primera vez y la exploración que se utilizó para descubrirla.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. Opcional: Busque los datos de vulnerabilidad.
4. Pulse la vulnerabilidad que desee investigar.
5. En la barra de herramientas, seleccione **Acciones** > **Historial**.

Tareas relacionadas:

"Buscar datos de vulnerabilidad" en la página 72
En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

Reducir el número de vulnerabilidades de falso positivo

En IBM Security QRadar Vulnerability Manager, puede crear automáticamente reglas de excepción para vulnerabilidades que están asociadas a un tipo de servidor determinado.

Cuando el usuario configura tipos de servidor, QRadar Vulnerability Manager crea reglas de excepción y automáticamente reduce las vulnerabilidades devueltas por la búsqueda de datos.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, seleccione **Descubrimiento de servidores**.
3. Para crear automáticamente reglas de excepción de falso positivo para vulnerabilidades asociadas a tipos de servidor determinados, seleccione una de las opciones siguientes en la lista **Tipo de servidor**:
   - Servidores FTP
   - Servidores DNS
   - Servidores de correo
   - Servidores web

   Pueden ser necesarios varios minutos para que se renueve el campo **Puertos**.
4. Opcional: En la lista **Red**, seleccione la red para los servidores.
5. Pulse **Descubrir servidores**.
6. En el panel Servidores coincidentes, seleccione los servidores donde se crean las reglas de excepción de vulnerabilidad.
7. Pulse **Aprobar servidores seleccionados**.

Resultados

Dependiendo del tipo de servidor seleccionado, las vulnerabilidades siguientes se establecen automáticamente como reglas de excepción de falso positivo:

Tabla 7. Vulnerabilidades de tipos de servidor

Tipo de servidor	Vulnerabilidad
Servidores FTP	**Servidor FTP presente**
Servidores DNS	**Servidor DNS en ejecución**
Servidores de correo	**Servidor SMTP detectado**
Servidores web	**Servicio web en ejecución**

Investigar activos y vulnerabilidades de alto riesgo

En IBM Security QRadar Vulnerability Manager, puede investigar vulnerabilidades de alto riesgo que pueden ser susceptibles de explotación.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la página Por instancias de vulnerabilidad, pulse la cabecera de columna **Puntuación de riesgo** para ordenar las vulnerabilidades de acuerdo con la puntuación de riesgo.
4. Para investigar las métricas de CVSS que se utilizan para obtener la puntuación de riesgo, pase el ratón sobre el campo **Puntuación de riesgo**.
5. Identifique la vulnerabilidad que tenga la puntuación de riesgo más alta y pulse el enlace **Vulnerabilidad**.
6. En la ventana Detalles de vulnerabilidad, investigue la vulnerabilidad:

a. Para ver el sitio web de IBM Security Systems, pulse el enlace **X-Force**.
b. Para ver el sitio web de la Base de datos nacional de vulnerabilidades, pulse el enlace **CVE**.

   El sitio web de IBM Security Systems y la Base de datos nacional de vulnerabilidades proporcionan información para corregir vulnerabilidades y detalles sobre cómo una vulnerabilidad puede afectar a su empresa.
c. Para abrir la ventana Aplicación de parches correspondiente a la vulnerabilidad, pulse el enlace **Detalles de plugin**. Utilice las pestañas para descubrir información preventiva de Oval Definition, Windows Knowledge Base o UNIX sobre la vulnerabilidad. Esta característica proporciona información sobre cómo QRadar Vulnerability Manager busca detalles de vulnerabilidad durante una exploración de parches. Puede utilizarla para identificar por qué ha surgido una vulnerabilidad en un activo o por qué no.
d. El cuadro de texto **Solución** contiene información detallada sobre cómo corregir una vulnerabilidad.

Conceptos relacionados:

"Detalles de puntuación de riesgo" en la página 71
En IBM Security QRadar Vulnerability Manager, las puntuaciones de riesgo de vulnerabilidad proporcionan una indicación del riesgo que una vulnerabilidad representa para su empresa.

Priorizar vulnerabilidades de alto riesgo mediante la aplicación de políticas de riesgo

En IBM Security QRadar Vulnerability Manager, puede alertar a los administradores respecto a las vulnerabilidades de alto riesgo aplicando políticas de riesgo a las vulnerabilidades.

Cuando aplica una política de riesgo a una vulnerabilidad, se ajusta la puntuación de riesgo de la vulnerabilidad, lo que permite que los administradores prioricen con más exactitud las vulnerabilidades que requieren atención inmediata.

En este ejemplo, la puntuación de riesgo de vulnerabilidad se incrementa automáticamente según un factor porcentual para cualquier vulnerabilidad que permanezca activa en la red después de 40 días.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
4. En el panel Parámetros de búsqueda, configure los filtros siguientes:
   a. **Riesgo es alto**
   b. **Días transcurridos desde que se descubrieron vulnerabilidades es mayor o igual que 40**
5. Pulse **Buscar** y luego pulse **Guardar criterios de búsqueda** en la barra de herramientas.

   Escriba un nombre de búsqueda guardada que sea identificable en QRadar Risk Manager.
6. Pulse la pestaña **Riesgos**.
7. En el panel de navegación, pulse **Supervisor de políticas**.

8. En la barra de herramientas, pulse **Acciones** > **Nuevo**.
9. En el campo **¿Qué nombre desea asignar a esta pregunta?**, escriba un nombre.
10. En el campo **¿Qué pruebas desea incluir en la pregunta?**, pulse **son susceptibles a vulnerabilidades contenidas en búsquedas guardadas de vulnerabilidades**.
11. En el campo **Buscar activos que**, pulse el parámetro subrayado en **son susceptibles a vulnerabilidades contenidas en búsquedas guardadas de vulnerabilidades**.
12. Identifique la búsqueda guardada de vulnerabilidades de alto riesgo de QRadar Vulnerability Manager, pulse **Añadir** y luego pulse **Aceptar**.
13. Pulse **Guardar pregunta**.
14. En el panel Preguntas, seleccione la pregunta en la lista y pulse **Supervisar** en la barra de herramientas.

    Restricción: El campo **Descripción de suceso** es obligatorio.
15. Pulse **Asignar sucesos pasados de pregunta**.
16. En el campo **Ajustes de puntuación de vulnerabilidad**, escriba un valor porcentual de ajuste de riesgo en el campo **Ajuste porcentual de puntuación de vulnerabilidad cuando no se pasa la pregunta**.
17. Pulse **Aplicar ajuste a todas las vulnerabilidades de un activo** y luego pulse **Guardar supervisor**.

Qué hacer a continuación

En el panel **Vulnerabilidades**, puede buscar vulnerabilidades de alto riesgo y priorizar las vulnerabilidades

Conceptos relacionados:

"Integración de QRadar Risk Manager y QRadar Vulnerability Manager" en la página 23
IBM Security QRadar Vulnerability Manager se integra con IBM Security QRadar Risk Manager para ayudarle a priorizar riesgos y vulnerabilidades en la red.

Tareas relacionadas:

"Guardar criterios de búsqueda de vulnerabilidades" en la página 77
En IBM Security QRadar Vulnerability Manager, puede guardar criterios de búsqueda de vulnerabilidades para su uso en el futuro.

Configurar colores personalizados para visualizar puntuaciones de riesgo

Configure colores personalizados para representar las puntuaciones de riesgo de IBM Security QRadar Vulnerability Manager en las interfaces de QRadar Vulnerability Manager.

Procedimiento

1. En IBM Security QRadar, seleccione **Vulnerabilidades** > **Asignación de vulnerabilidades** > **Preferencias de riesgo**.
2. En la columna **Mayor o igual que**, escriba la puntuación de riesgo mínima para Alto, Medio, Bajo, y Aviso.
3. En la columna **Color**, seleccione o defina un color para representar las puntuaciones de riesgo Alto, Medio, Bajo, y Aviso.

Identificar vulnerabilidades para las que existe un parche de BigFix

En IBM Security QRadar Vulnerability Manager, puede identificar las vulnerabilidades para las que existe un arreglo.

Después de identificar las vulnerabilidades para las que existe un arreglo, puede investigar información detallada sobre arreglos en la ventana Detalles de vulnerabilidad.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**
4. En el panel Parámetros de búsqueda, configure las opciones siguientes:
   a. En la **primera lista** seleccione **Referencia externa de tipo**.
   b. En la **segunda lista**, seleccione **Igual que**.
   c. En la **tercera lista**, seleccione **Parche de IBM BigFix**.
   d. Pulse **Añadir filtro**.
   e. Pulse **Buscar**.

      La página Por instancias de vulnerabilidad muestra las vulnerabilidades que tienen un arreglo disponible.
5. Opcional: Ordene las vulnerabilidades de acuerdo con su importancia pulsando la cabecera de columna **Puntuación de riesgo**.
6. Opcional: Para investigar información sobre parches para una vulnerabilidad, pulse un enlace de vulnerabilidad en la columna **Vulnerabilidad**.
7. Opcional: En la ventana Detalles de vulnerabilidad, vaya al final de la ventana para ver la información sobre parches de vulnerabilidad.

   ID de sitio e **ID de fixlet** son identificadores exclusivos que se utilizan para aplicar parches de vulnerabilidad mediante IBM BigFix.

   La columna **Base** indica una referencia exclusiva que puede utilizar para acceder a más información contenida en una base de conocimientos.

Identificar el estado de parche de las vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede identificar el estado de parche de las vulnerabilidades.

Mediante el filtrado de las vulnerabilidades con parche, puede dar prioridad a la corrección de las vulnerabilidades más críticas de la empresa.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. En la ventana **primera lista** del panel Parámetros de búsqueda, seleccione **Estado de parche**.
5. En la **segunda lista**, seleccione un modificador de búsqueda.
6. Para filtrar las vulnerabilidades de acuerdo con su estado de parche, seleccione una de las opciones siguientes en la tercera lista:

Opción	Descripción
Descargas pendientes	Seleccione esta opción para mostrar las vulnerabilidades para las que se planificado la aplicación de un parche
Reinicio pendiente	Seleccione esta opción para mostrar las vulnerabilidades a las que se aplica un parche después de reiniciar el activo explorado
Corregido	Seleccione esta opción para mostrar las vulnerabilidades a las que IBM BigFix ha aplicado un parche

7. Pulse **Añadir filtro**.
8. Pulse **Buscar**.

Conceptos relacionados:

"Integración de BigFix" en la página 24
IBM Security QRadar Vulnerability Manager se integra con IBM BigFix para ayudarle a filtrar y priorizar las vulnerabilidades que se pueden corregir.

Eliminación de los datos de vulnerabilidad no deseados

Utilice las funciones de limpieza de vulnerabilidades de QRadar Vulnerability Manager para eliminar los datos de vulnerabilidad obsoletos del modelo de activos.

Acerca de esta tarea

Cualquiera de los escenarios siguientes puede generar datos de vulnerabilidad no deseados:

- Cambio del tipo de explorador
- Activos fuera de servicio
- Cambio de dirección IP
- Exploraciones inexactas o de prueba

Importante: Una vez eliminados los datos de vulnerabilidad correspondientes a un tipo de explorador o activo, no se pueden recuperar.

Procedimiento

Para eliminar los datos de vulnerabilidad no deseados, tiene dos opciones:

- Utilice la página **Acciones** > **Limpiar vulnerabilidades (Todas)** de la página Activos para eliminar todos los datos de vulnerabilidad correspondientes a un tipo de explorador seleccionado.
- Utilice la página **Acciones** > **Limpiar vulnerabilidades (Activos)** de la página Activos para eliminar todos los datos de vulnerabilidad correspondientes a un activo determinado con un tipo de explorador seleccionado.

Configuración de periodos de retención de datos de vulnerabilidad

Puede establecer el periodo de retención para los datos de tendencia de vulnerabilidad y los resultados de exploración en la ventana Configuración del perfilador de activos.

Acerca de esta tarea

Utilice las reglas de configuración en la sección **Retención de vulnerabilidad de QVM** de la ventana Configuración del perfilador de activos para definir cuánto tiempo conserva IBM Security QRadar Vulnerability Manager los datos de tendencia de vulnerabilidad y los resultados de exploración.

Procedimiento

1. Pulse **Admin** > **Configuración del perfilador de activos**.
2. En la sección **Retención de vulnerabilidad de QVM** de la ventana Configuración del perfilador de activos, escriba un valor en los campos siguientes:

Regla	Descripción	Valor predet,
Datos de creación de informes de tendencia de vulnerabilidad (en días)	Establece cuántos días QRadar Vulnerability Manager conserva los datos de tendencia de vulnerabilidad para su uso en los informes de vulnerabilidades diarios.	14 días
Datos de creación de informes de tendencia de vulnerabilidad (en semanas)	Establece cuántas semanas QRadar Vulnerability Manager conserva los datos de tendencia de vulnerabilidad para su uso en los informes de vulnerabilidades semanales.	14 semanas
Datos de creación de informes de tendencia de vulnerabilidad (en meses)	Establece cuántos meses QRadar Vulnerability Manager conserva los datos de tendencia de vulnerabilidad para su uso en los informes de vulnerabilidades mensuales.	14 meses
Depurar resultados de exploración después de periodo (en días)	Utilice esta regla con **Depurar resultados de exploración después de periodo (en ciclos de ejecución)** para establecer los límites de retención para los datos de resultados de exploración. Establece el número de días que QRadar Vulnerability Manager conserva los datos después de que aplicar la regla de limitación **Depurar resultados de exploración después de periodo (en ciclos de ejecución)**.	30 días

Regla	Descripción	Valor predet,
Depurar resultados de exploración después de periodo (en ciclos de ejecución)	Utilice esta regla con **Depurar resultados de exploración después de periodo (en días)** para establecer los límites de retención para los datos de resultados de exploración. Establece cuántas versiones de los datos de resultados de exploración conserva QRadar Vulnerability Manager. Esta regla tiene prioridad sobre el valor que establezca en **Depurar resultados de exploración después de periodo (en días)**. Para los valores predeterminados de las reglas **Depurar resultados de exploración después de periodo (en días)** y **Depurar resultados de exploración después de periodo (en ciclos de ejecución)**: • QRadar Vulnerability Manager conserva los datos de resultados de exploración de los tres ciclos de ejecución más recientes. También conserva cualquier otra versión de los resultados de las exploraciones que se ejecuten dentro del límite de 30 días. • Si alguno de los tres ciclos de ejecución más recientes se han producido después del límite de 30 días, QRadar Vulnerability Manager conserva los datos de resultados de exploración de esos ciclos de ejecución.	Tres ciclos de ejecución

3. Pulse **Guardar**.

Capítulo 8. Reglas de excepción de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede configurar reglas de excepción para reducir el número de vulnerabilidades de falso positivo.

Puede aplicar reglas de excepción a vulnerabilidades para reducir el número de vulnerabilidades que se muestran en los resultados de búsqueda.

Si crea una excepción de vulnerabilidad, la vulnerabilidad no se elimina de QRadar Vulnerability Manager.

Ver reglas de excepción

Para ver excepciones de vulnerabilidad, puede buscar datos de vulnerabilidad mediante filtros de búsqueda.

Para ver reglas de excepción, pulse la pestaña **Vulnerabilidades** y luego pulse **Excepción de vulnerabilidad** en el panel de navegación.

Tareas relacionadas:

"Reducir el número de vulnerabilidades de falso positivo" en la página 79
En IBM Security QRadar Vulnerability Manager, puede crear automáticamente reglas de excepción para vulnerabilidades que están asociadas a un tipo de servidor determinado.

Aplicar una regla de excepción de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede aplicar manualmente una regla de excepción a una vulnerabilidad para la cual determine que no representa una amenaza importante.

Si aplica una regla de excepción, la vulnerabilidad ya no aparece en los resultados de búsqueda de QRadar Vulnerability Manager. Pero la vulnerabilidad no se elimina de QRadar Vulnerability Manager.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Gestionar vulnerabilidades** > **Por red**.
3. Opcional: Busque los datos de vulnerabilidad. En la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
4. Pulse el enlace de la columna **Instancias de vulnerabilidad**.
5. Seleccione la vulnerabilidad para la que desee crear una regla de excepción.
6. En la barra de herramientas, seleccione **Acciones** > **Excepción**.

   Para aplicar una regla de excepción de vulnerabilidad, el único campo obligatorio es el cuadro de texto **Comentario**. Todos los demás parámetros son opcionales.
7. Opcional: En la ventana Mantener regla de excepción, elija una de las opciones siguientes:
   - Escriba una fecha en la que debe caducar la excepción de vulnerabilidad.
   - Si la excepción de vulnerabilidad no debe caducar nunca, pulse **No caduca nunca**.

8. En la sección Notas de la ventana Mantener regla de excepción, escriba texto en el cuadro de texto **Comentarios**.
9. Pulse **Guardar**.

Tareas relacionadas:

"Buscar datos de vulnerabilidad" en la página 72
En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

Gestionar una regla de excepción de vulnerabilidad

Si recibe información nueva sobre una vulnerabilidad, puede actualizar o eliminar una regla de excepción de vulnerabilidad existente.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Excepción de vulnerabilidad**.
3. Pulse la vulnerabilidad que desee gestionar.
4. En la barra de herramientas, seleccione una opción del menú **Acciones**.

   Importante: Si suprime una regla de excepción de vulnerabilidad, no se visualiza ningún aviso. La vulnerabilidad se suprime inmediatamente.
5. Pulse **Guardar**.

Buscar excepciones de vulnerabilidad

En IBM Security QRadar Vulnerability Manager, puede buscar datos de vulnerabilidad y filtrar los resultados de búsqueda para mostrar excepciones de vulnerabilidad.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Gestionar vulnerabilidades** > **Por activo**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. Para filtrar los datos de vulnerabilidad a fin de incluir excepciones de vulnerabilidad, seleccione una de las opciones siguientes en el panel Parámetros de búsqueda:
   - Incluir excepciones de vulnerabilidad

     Muestra todas las vulnerabilidades, incluidas las vulnerabilidades que tienen una regla de excepción aplicada a ellas.
   - Incluir solo excepciones de vulnerabilidad

     Muestra solo las vulnerabilidades que tienen una regla de excepción aplicada a ellas.
5. Pulse **Añadir filtro**.
6. Pulse **Buscar**.

Capítulo 9. Corrección de vulnerabilidades

En QRadar Vulnerability Manager, puede asignar vulnerabilidades a un usuario técnico para su corrección.

Puede asignar vulnerabilidades a un usuario técnico utilizando dos métodos.

- Asigne vulnerabilidades individuales a un usuario técnico para su corrección.
- Asigne un usuario técnico como propietario de grupos de activos

Tareas relacionadas:

"Configurar tiempos de corrección para las vulnerabilidades en activos asignados" en la página 91
En IBM Security QRadar Vulnerability Manager, puede configurar tiempos de corrección para diferentes tipos de vulnerabilidades.

Asignar vulnerabilidades individuales a un usuario técnico para corregirlas

En IBM Security QRadar Vulnerability Manager, puede asignar vulnerabilidades individuales a un usuario de QRadar para corregirlas.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Gestionar vulnerabilidades**.
3. Opcional: Busque los datos de vulnerabilidad.
4. Seleccione la vulnerabilidad que desee asignar para corregirla.
5. En la barra de herramientas, pulse **Acciones** > **Asignar/editar**.
6. Seleccione un usuario técnico en la lista **Usuario asignado**.

   Los usuarios técnicos se asignan en la página Asignación de vulnerabilidades. Para obtener más información, consulte "Asignar un usuario técnico como propietario de grupos de activos".
7. Opcional: En la lista **Fecha de vencimiento**, seleccione una fecha futura en la que se debe corregir la vulnerabilidad.

   Si no selecciona una fecha, el campo **Fecha de vencimiento** toma como valor la fecha actual.
8. Opcional: En el campo **Notas**, escriba información útil sobre la razón de la asignación de la vulnerabilidad.
9. Pulse **Guardar**.

Asignar un usuario técnico como propietario de grupos de activos

En IBM Security QRadar Vulnerability Manager puede configurar grupos de activos y asignar automáticamente sus vulnerabilidades a usuarios técnicos.

Después de asignar un usuario técnico y explorar los activos, todas las vulnerabilidades existentes en los activos se asignan al usuario técnico para corregirlas.

Las horas de corrección de las vulnerabilidades se pueden configurar mediante la opción **Horas de remediación**, dependiendo del riesgo o gravedad.

Si añade un nuevo activo a la red y éste pertenece al grupo de activos de un usuario técnico, las vulnerabilidades del activo se asignan automáticamente al usuario técnico.

Puede enviar automáticamente por correo electrónico informes a los usuarios técnicos con detalles de las vulnerabilidades que están encargados de corregir.

Las opciones **Horas de remediación**, **Planificar** y **Preferencias de riesgo** sólo están habilitadas para los usuarios administrativos, y para los usuarios no administrativos que no tienen ningún dominio asociado.

Antes de empezar

Si desea configurar un grupo de activos que se identifican mediante una búsqueda de activos guardada, debe buscar los activos y guardar los resultados.

Para obtener más información sobre buscar activos y guardar los resultados, consulte la *Guía del usuario* del producto.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Asignación de vulnerabilidades**.
3. En la barra de herramientas, pulse **Añadir**.
4. Escriba un nombre, dirección de correo electrónico, y rango de CIDR.

   Para asignar automáticamente un usuario técnico en la ventana Nuevo propietario de activo, los únicos campos obligatorios son **Nombre**, **Correo electrónico** y **CIDR**. Si los entornos multidominio están habilitados, seleccione una asociación de dominio para ese propietario de activo en particular.
5. Si ha configurado IBM Security QRadar para varios dominios, seleccione el dominio correspondiente en la lista **Dominio**.
6. Para filtrar la lista de los activos comprendidos en el rango de CIDR de acuerdo con el nombre del activo, escriba una serie de texto en el campo **Filtro de nombres de activos**.
7. Para filtrar la lista de los activos comprendidos en el rango de CIDR de acuerdo con el sistema operativo, escriba una serie de texto en el campo **Filtro de sistemas operativos**.
8. Opcional: Para asignar el usuario técnico a los activos que están asociados con una búsqueda de activos guardada, pulse **Búsqueda de activo**. La opción **Búsqueda de activo** está inhabilitada si se han configurado dominios en la página Gestión de dominios.
9. Pulse **Guardar**.
10. Opcional: En la barra de herramientas, pulse **Tiempos de corrección**.

    Puede configurar el tiempo de corrección para cada tipo de vulnerabilidad, de acuerdo con su riesgo y gravedad.

    Puede ejemplo, puede desear que las vulnerabilidades de alto riesgo se corrijan en el transcurso de 5 días.
11. Opcional: En la barra de herramientas, pulse **Planificar**.

    De forma predeterminada, el contacto de usuario técnico para activos se actualiza cada 24 horas.

Los activos nuevos añadidos al entorno que estén dentro del rango de CIDR especificado se actualizan automáticamente con el contacto técnico que ha especificado.

Importante: La planificación se aplica a las asociaciones que ha creado entre técnicos usuarios y grupos de activos.

12. Opcional: Pulse **Actualizar ahora** para establecer inmediatamente el propietario de los activos.

    Dependiendo del tamaño del despliegue, puede ser necesario un periodo de tiempo largo para actualizar los activos.

13. Pulse **Guardar**.

    Todas las vulnerabilidades que ya están asignados a un usuario técnico para corregirlas se actualizan con el nuevo usuario técnico.

14. Si previamente no se han asignado vulnerabilidades a un usuario técnico, debe explorar los activos que asignó al usuario técnico.

    Importante: La exploración de activos verifica que las vulnerabilidades asignadas a un usuario técnico existen en el activo.

Configurar tiempos de corrección para las vulnerabilidades en activos asignados

En IBM Security QRadar Vulnerability Manager, puede configurar tiempos de corrección para diferentes tipos de vulnerabilidades.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Asignación de vulnerabilidades**.
3. Seleccione una asignación en la lista Propietarios de activos.
4. En la barra de herramientas, pulse **Tiempos de corrección**.
5. Actualice los tiempos de corrección para las vulnerabilidades de acuerdo con su riesgo y gravedad.
6. Pulse **Guardar**.

Capítulo 10. Informes de vulnerabilidades

En IBM Security QRadar Vulnerability Manager, puede crear un informe o editar un informe existente, o utilizar el asistente de informes para crear, planificar o distribuir un informe nuevo.

QRadar Vulnerability Manager contiene varios informes predeterminados.

El asistente de informes proporciona una guía paso a paso sobre cómo diseñar, planificar y generar informes.

Para obtener más información, consulte el manual *IBM Security QRadar SIEM Users Guide*.

Envío por correo electrónico a usuarios técnicos de vulnerabilidades asignadas que necesitan corrección

Cuando asigna vulnerabilidades a un usuario técnico para su corrección, puede crear un informe que envía un correo electrónico al usuario técnico.

El correo electrónico contiene información sobre las vulnerabilidades que el usuario técnico debe corregir.

Crear informes de conformidad de PCI

Puede crear un informe de conformidad para activos de PCI (sector de las tarjetas de pago).

El informe de conformidad demuestra que se han tomado todas las precauciones de seguridad necesarias para proteger activos críticos.

Ejecutar un informe predeterminado de QRadar Vulnerability Manager

En IBM Security QRadar Vulnerability Manager, puede ejecutar un informe de gestión de vulnerabilidades predeterminado.

Procedimiento

1. Pulse la pestaña **Informes**.
2. En la lista de informes, seleccione el informe que desea ejecutar.

   Por ejemplo, puede mostrar un informe general de vulnerabilidades correspondiente a los últimos siete días.
3. En la barra de herramientas, seleccione **Acciones** > **Ejecutar informe** y luego pulse **Aceptar**.
4. Para ver el informe completado en formato PDF, pulse el icono contenido en la columna **Formatos**.

Enviar por correo electrónico informes de vulnerabilidades asignadas a usuarios técnicos

En IBM Security QRadar Vulnerability Manager, puede enviar un informe de vulnerabilidades asignadas al contacto técnico para cada activo.

El informe enviado informa a los administradores de que tienen vulnerabilidades asignadas que necesitan corrección. Los informes se pueden planificar para ser enviados cada mes, cada semana, cada día o cada hora.

Antes de empezar

Debe realizar las tareas siguientes:

1. Asignar un usuario técnico como propietario de grupos de activos. Para obtener más información, consulte "Asignar un usuario técnico como propietario de grupos de activos" en la página 89.
2. Explorar los activos que ha asignado el propietario técnico.
3. Crear y guardar una búsqueda de vulnerabilidades que utiliza el parámetro **Contacto de propietario técnico** como dato de entrada. Para obtener más información, consulte "Buscar datos de vulnerabilidad" en la página 72.

Procedimiento

1. Pulse la pestaña **Informes**.
2. En la barra de herramientas, seleccione **Acciones** > **Crear**.
3. Pulse **Semanal** y luego pulse **Siguiente**.
4. Pulse en el diseño de informe no dividido que se muestra en la sección superior izquierda del asistente de informes y pulse **Siguiente**.
5. Escriba un **Título de informe**.
6. En la lista **Tipo de gráfico**, seleccione **Vulnerabilidades de activos** y escriba un **Título de gráfico**.
7. Opcional: Si un contacto de propietario técnico tiene asignados más de cinco activos y desea enviar por correo electrónico toda la información sobre activos, aumente el valor en la lista **Limitar activos a primeros**.

   Recuerde: Utilice la pestaña **Activos** para comprobar que un mismo contacto de propietario técnico está asignado a cada activo del cual es responsable.
8. En el campo **Tipo de gráfico** , seleccione **AggregateTable**.

   Si selecciona un valor distinto de **AggregateTable**, el informe no genera un subinforme de vulnerabilidades.
9. En el panel Contenido de gráfico, pulse **Búsqueda para utilizar**, seleccione la búsqueda de vulnerabilidades de contacto técnico y pulse **Guardar detalles de contenedor**.
10. Pulse **Siguiente** y seleccione el tipo de salida del informe.
11. En la sección de distribución de informes del asistente de informes, pulse **Varios informes**.
12. Pulse **Todos los propietarios de activos**.
13. Opcional: Pulse **Cargar propietarios de activos** para ver la lista completa de detalles de contactos de usuarios técnicos.

    Puede eliminar los usuarios técnicos a los que no desee enviar por correo electrónico una lista de vulnerabilidades asignadas.
14. En la lista Informes, seleccione el informe que ha creado, y en la barra de herramientas, seleccione **Acciones** > **Ejecutar informe**.

Tareas relacionadas:

"Asignar un usuario técnico como propietario de grupos de activos" en la página 89

En IBM Security QRadar Vulnerability Manager puede configurar grupos de activos y asignar automáticamente sus vulnerabilidades a usuarios técnicos.

"Buscar datos de vulnerabilidad" en la página 72
En IBM Security QRadar Vulnerability Manager, puede identificar vulnerabilidades importantes buscando datos de vulnerabilidad.

Crear informes de conformidad de PCI

En IBM Security QRadar Vulnerability Manager, puede crear un informe de conformidad para activos de PCI (sector de las tarjetas de pago). Por ejemplo, crear un informe para activos que almacenan información sobre tarjetas de crédito u otra información financiera confidencial.

El informe de conformidad demuestra que el usuario ha tomado todas las precauciones de seguridad necesarias para proteger sus activos.

Procedimiento

1. Ejecute una exploración de PCI para los activos de la red que almacenan o procesan información de PCI.

   Para obtener más información, consulte "Crear un perfil de exploración" en la página 31.
2. Actualice las declaraciones de planes de conformidad de activos y de software

   Las declaraciones de planes de conformidad y de software se muestran en la sección de notas especiales del resumen ejecutivo.

   Para obtener más información, consulte los estándares de seguridad PCI para proveedores de software autorizados.
3. Cree y ejecute un informe de conformidad de PCI para los activos que ha explorado.

Tareas relacionadas:

"Crear un perfil de exploración" en la página 31
En IBM Security QRadar Vulnerability Manager, puede configurar perfiles de exploración para especificar cómo y cuándo se exploran los activos de la red para buscar vulnerabilidades.

Actualizar declaraciones de planes de conformidad de activos y de software

En IBM Security QRadar Vulnerability Manager, si desea generar un informe de conformidad de PCI para activos, debe completar declaraciones de conformidad para cada activo.

La declaración de conformidad se muestra en el informe de conformidad de PCI.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activos**.
3. En la página Activos, seleccione el activo para el que desee proporcionar una declaración de conformidad.
4. En la barra de herramientas, pulse **Editar activo**.
5. En la ventana Editar perfil de activo, pulse el panel **CVSS, peso y conformidad**.
6. Complete los campos siguientes. Utilice la ayuda contextual si necesita ayuda:
   - Plan de conformidad
   - Notas de conformidad

- Declaración de notas de conformidad
- Descripción de notas de conformidad
- Razón de conformidad fuera de ámbito

7. Pulse **Guardar**.

Crear un informe de conformidad de PCI

En IBM Security QRadar Vulnerability Manager, puede crear y ejecutar un informe de conformidad de PCI.

El informe de conformidad de PCI demuestra que los activos que intervienen en actividades de PCI cumplen las precauciones de seguridad que impiden ataques externos.

Antes de empezar

Asegúrese de que ha ejecutado una exploración de conformidad de PCI.

Procedimiento

1. Pulse la pestaña **Informes**.
2. En la barra de herramientas, seleccione **Acciones** > **Crear**.
3. Pulse **Semanal** y luego pulse **Siguiente**.
4. Pulse en el diseño de informe no dividido que se muestra en la sección superior izquierda del asistente de informes y pulse **Siguiente**.
5. Escriba un **Título de informe**.
6. En la lista **Tipo de gráfico**, seleccione **Conformidad de vulnerabilidad** y escriba un **Título de gráfico**.
7. En la lista **Perfil de exploración**, seleccione el perfil de exploración para los activos que exploró.

   Atención: Si no se muestra ningún perfil de exploración, debe crear y ejecutar una exploración de PCI para los activos de la red que almacenan o procesan información de PCI.
8. En la lista **Resultado de exploración**, seleccione la versión del perfil de exploración que desee utilizar.

   Recuerde: Para proporcionar evidencia de cumplimiento, debe seleccionar la opción **Más reciente** en la lista **Resultado de exploración**. También puede generar un informe de conformidad utilizando un perfil de exploración que se ejecutó en una fecha anterior.
9. En la lista **Tipo de informe**, seleccione un tipo de informe.

   Si selecciona **Resumen ejecutivo**, **Detalles de vulnerabilidad** o una combinación de ambos, la declaración de conformidad se asocia automáticamente al informe de conformidad de PCI.
10. Complete la información de los paneles **Información de cliente de exploración** e **Información de proveedor de exploración aprobada**.

    Importante: Debe añadir un nombre en el campo **Empresa** de ambos paneles, pues esta información se visualiza en la sección de declaración de conformidad del informe.
11. Pulse **Guardar detalles de contenedor** y luego pulse **Siguiente**.
12. Utilice el Asistente de informes para completar el informe de conformidad de PCI.

Resultados

El informe aparecerá en la lista de informes y se creará automáticamente.

Incluir cabeceras de columna en las búsquedas de activos

Puede limitar las búsquedas de activos con filtros que incluyen perfiles de activo personalizados, nombre, recuento de vulnerabilidades y puntuación de riesgo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activos**, y en la barra de herramientas, pulse **Buscar** > **Búsqueda nueva**.
3. En el campo del lado izquierdo que contiene nombres de columna, pulse las cabeceras de columna que desee incluir en la búsqueda y pulse el botón de flecha para trasladar las cabeceras seleccionadas al campo situado en el lado derecho.
4. Pulse los botones de flecha arriba y flecha abajo para cambiar la prioridad de las cabeceras de columna seleccionadas.
5. Cuando el campo del lado derecho contenga todas las cabeceras de columna para las que desee buscar, pulse **Buscar**.

Capítulo 11. Investigación, noticias y avisos sobre vulnerabilidades

Puede utilizar IBM Security QRadar Vulnerability Manager para seguir informado sobre el nivel de amenaza de las vulnerabilidades y gestionar la seguridad en su empresa.

Una biblioteca de vulnerabilidades contiene vulnerabilidades habituales que se recopilan a partir de una lista de fuentes externas. El recurso externo más importante es la Base de datos nacional de vulnerabilidades (NVD). Puede investigar vulnerabilidades determinadas utilizando varios criterios, tales como proveedor, producto y rango de fechas. Puede estar interesado en vulnerabilidades específicas que existen en productos o servicios utilizados en su empresa.

QRadar Vulnerability Manager también proporciona una lista de artículos y avisos relacionados con la seguridad que se han recogido a partir de una lista externa de recursos y proveedores. Los artículos y avisos son una fuente útil de información de seguridad procedente de todo el mundo. Los artículos también le ayudan a tener información actualizada sobre riesgos de seguridad actuales.

Ver información detallada sobre vulnerabilidades publicadas

En IBM Security QRadar Vulnerability Manager, puede ver información detallada sobre vulnerabilidades.

En la página Investigar vulnerabilidades, puede investigar métricas de CVSS y acceder a información de investigación y desarrollo de IBM X-Force.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, seleccione **Investigar** > **Vulnerabilidades**.
3. Opcional: Si no se visualiza ninguna vulnerabilidad, seleccione un rango de tiempo alternativo en la lista **Ver vulnerabilidades desde**.
4. Opcional: Para buscar vulnerabilidades, en la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
5. Identifique la vulnerabilidad que desee investigar.
6. Pulse el enlace de vulnerabilidad en la columna **Nombre de vulnerabilidad**.

Seguir informado sobre noticias referentes a la seguridad global

En IBM Security QRadar Vulnerability Manager, puede ver noticias de seguridad de todo el mundo para ayudarle a estar al día de las novedades actuales sobre seguridad.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Investigar** > **Noticias**.
3. Si no se muestra ningún artículo de noticias, seleccione un rango de tiempo alternativo en la lista **Ver noticias desde**.

4. Para buscar artículos de noticias, en la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
5. Identifique el artículo de noticias que desee investigar.
6. Pulse el enlace de artículo de noticias en la columna **Título del artículo**.

Ver avisos de seguridad de los proveedores de software

En IBM Security QRadar Vulnerability Manager, puede ver avisos sobre vulnerabilidades que son emitidos por proveedores de software. Utilice la información de aviso para identificar riesgos en la tecnología utilizada y conocer las implicaciones del riesgo.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Investigar** > **Avisos**.
3. Si no se visualiza ningún aviso, seleccione un rango de tiempo alternativo en la lista **Ver avisos desde**.
4. Si desea buscar avisos de seguridad, en la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
5. Pulse el enlace de aviso en la columna **Aviso**.

   Cada aviso de seguridad puede incluir referencias, soluciones y procedimientos alternativos para vulnerabilidades.

Buscar vulnerabilidades, noticias y avisos

En IBM Security QRadar Vulnerability Manager, puede buscar las noticias y avisos más recientes que los proveedores de software publican sobre vulnerabilidades.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse una de las opciones siguientes:
   - **Investigar** > **Vulnerabilidades**.
   - **Investigar** > **Noticias**.
   - **Investigar** > **Avisos**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. Escriba una frase de búsqueda en el campo **Frase**.
5. Si está buscando noticias, seleccione una fuente de noticias en la lista **Fuente**.
6. En el área **Por rango de fechas**, especifique el periodo de fechas de las noticias o avisos en los que esté interesado.
7. Si está buscando una vulnerabilidad publicada, especifique un proveedor, un producto y una versión de producto en el área **Por producto**.
8. Si está buscando una vulnerabilidad publicada, especifique un ID de CVE, Vulnerabilidad u OSVDB en el área **Por ID**.

Canales de información de noticias

Utilice los elementos del panel de control **Canales de información RSS** para ver las noticias más recientes sobre seguridad de IBM, consejos, información sobre vulnerabilidades publicada y actualizaciones de exploraciones que se han completado o que están en curso.

El elemento del panel de control **Canales de información RSS** va mostrando los resultados de exploración y las diez noticias más recientes de forma rotativa para que no tenga que buscar la información en las páginas Investigar ni Resultados de la exploración de la pestaña **Vulnerabilidades**.

En la pestaña **Panel de control**, utilice el menú **Añadir elemento** > **Informes** > **Canales de información RSS** para añadir canales de información RSS al panel de control.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Pero corresponde al usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 EE.UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O ADECUACIÓN PARA UN FIN DETERMINADO. Algunas legislaciones no permiten la renuncia de garantías expresas ni implícitas en determinadas transacciones, por lo que es posible que esta declaración no sea aplicable en su caso.

Esta información puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de estos sitios web. La información de esos sitios web no forman parte de la información del presente producto de IBM y el uso de esos sitios web se realiza bajo la responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los licenciatarios de este programa que deseen tener información sobre él para permitir: (i) el intercambio de información entre programas creados por separado y otros programas (incluido el presente) y (ii) el uso mutuo de la información intercambiada, se deben poner en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, EE.UU.

Esta información puede estar disponible, sujeta a los términos y condiciones apropiados, incluido, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos en este documento se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Algunas mediciones se han realizado en sistemas a nivel de desarrollo y no es seguro que estas mediciones serán las mismas en los sistemas de uso general. Además, algunas mediciones se han calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios del presente documento deben verificar los datos aplicables correspondientes al entorno específico utilizado.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las preguntas referentes a prestaciones de productos que no son de IBM se debe dirigir a los proveedores de esos productos.

Todas las declaraciones relativas a la orientación o intención futura de IBM están sujetas a cambio o anulación sin previo aviso y representan solamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

La presente información contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios. Cualquier similitud con los nombres y direcciones utilizados por una empresa real es completamente accidental.

Si está viendo la presente información en forma de copia software, las fotografías y figuras en color pueden no ser visibles.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

Java y todas las marcas registradas y los logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otras empresas.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio, (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia final del usuario, adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se proporciona información específica sobre el uso de cookies de esta oferta.

Dependiendo de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que obtienen el ID de sesión de cada usuario para gestionar y autenticar la sesión. Estos cookies se pueden inhabilitar, pero si se inhabilitan, también se elimina la funcionalidad que los cookies hacen posible.

Si las configuraciones desplegadas para esta Oferta de software le proporcionan como cliente la capacidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, lo cual incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías para estos fines, incluidos los cookies, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.

Glosario

Este glosario proporciona términos y definiciones para el software y productos de IBM Security QRadar Vulnerability Manager.

En este glosario se utilizan las referencias cruzadas siguientes:

- *Véase* le remite desde un término no preferido al término preferido o desde una abreviatura a la forma completa.
- *Véase también* le remite a un término relacionado u opuesto.

Para otros términos y definiciones, consulte el sitio web de IBM Terminology (se abre en una ventana nueva).

A

activo Objeto gestionable que se ha desplegado o que se debe desplegar en un entorno operativo.

alta disponibilidad (HA)
Relativo a un sistema dispuesto en clúster que se reconfigura cuando se producen errores de nodo o de daemon para que las cargas de trabajo se puedan redistribuir hacia los nodos restantes del clúster.

aviso Documento que contiene información y análisis acerca de una amenaza o vulnerabilidad.

B

base de datos nacional de vulnerabilidades (NVD)
Repositorio de datos de gestión de vulnerabilidades basados en estándares situado en Estados Unidos.

C

CDP Véase posibilidad de daño colateral.

CIDR Véase Classless Inter-Domain Routing.

cifrado
En seguridad informática, proceso de transformar datos en un formato ininteligible de manera que no se puedan obtener los datos originales o sólo se puedan obtener utilizando un proceso de descifrado.

Classless Inter-Domain Routing (CIDR)
Método para añadir direcciones de Protocolo Internet (IP) de la clase C. Las direcciones se proporcionan a los proveedores de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y permiten la existencia de más direcciones IP disponibles dentro de las empresas.

cliente
Programa de software o sistema que solicita servicios a un servidor.

Common Vulnerability Scoring System (CVSS)
Sistema de puntuación para medir la gravedad de una vulnerabilidad.

consola
Interfaz basada en la web desde la que un operador puede controlar y observar el funcionamiento del sistema.

CVSS Véase Common Vulnerability Scoring System.

D

delito Mensaje enviado o suceso generado en respuesta a una condición supervisada. Por ejemplo, un delito proporcionará información sobre si se ha vulnerado una política o la red está bajo ataque.

DNS Véase Sistema de nombres de dominio.

E

exploración bajo demanda
Exploración que sólo se ejecuta cuando es iniciada por el usuario. Los tipos de exploraciones incluyen exploraciones completas, exploraciones de descubrimiento, exploraciones de parches, exploraciones de PCI, exploraciones de bases de datos y exploraciones de web.

H

HA Véase alta disponibilidad.

I

intervalo operativo
Periodo de tiempo configurado dentro del cual se puede ejecutar una exploración.

IP Véase Protocolo Internet.

L

lista de exclusiones de exploración
Lista de activos, grupos de red y rangos de CIDR que se pasan por alto en las exploraciones.

N

Nivel de gravedad de PCI
Nivel de riesgo que una vulnerabilidad representa para a la industria de las tarjetas de pago.

NVD Véase base de datos nacional de vulnerabilidades.

P

Payment Card Industry Data Security Standard (PCI DSS)
Estándar mundial de seguridad de la información elaborado por PCI SSC (Payment Card Industry Security Standards Council). El estándar se creó para ayudar a las empresas que procesan pagos con tarjeta a impedir el fraude en las tarjetas de crédito mediante mayores controles en los datos y en su exposición al riesgo. El estándar se aplica a todas las empresas que contienen, procesan o pasan información sobre titulares de tarjetas que tengan el logotipo de alguna de las marcas de tarjeta.

PCI DSS
Véase Payment Card Industry Data Security Standard.

perfil de exploración
Información de configuración que especifica cómo y cuándo se exploran los activos de una red en busca de vulnerabilidades.

posibilidad de daño colateral (CDP)
Medida del posible efecto de una vulnerabilidad explotada sobre un activo físico o una empresa.

proceso de remediación
Proceso de asignar, supervisar y corregir las vulnerabilidades que se han identificado en un activo.

Protocolo de control de transmisiones (TCP)
Protocolo de comunicación utilizado en Internet y en todas las redes que siguen los estándares de la IETF (Internet Engineering Task Force) para el protocolo de interconexión de redes. TCP proporciona un protocolo fiable de host a host en redes de comunicación de conmutación de paquetes y en sistemas interconectados de esas redes. Véase también Protocolo Internet.

Protocolo Internet (IP)
Protocolo que direcciona datos a través de una red o redes interconectadas. Este protocolo actúa como intermediario entre las capas de protocolo superiores y la red física. Vea también Protocolo de control de transmisiones.

Protocolo simple de gestión de red (SNMP)
Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. La información sobre dispositivos gestionados se define y almacena en una Base de información de gestión (MIB).

R

regla de excepción de falso positivo
Regla específica de vulnerabilidades de bajo riesgo que minimiza el volumen de vulnerabilidades que se gestionan.

S

Sistema de nombres de dominio (DNS)
Sistema de bases de datos distribuidas que correlaciona nombres de dominio con direcciones IP.

SNMP
Véase Protocolo simple de gestión de red.

T

TCP Véase Protocolo de control de transmisiones.

transferencia de zona de DNS
Transacción que replica una base de datos de Sistema de nombres de dominio (DNS).

U

UDP Véase User Datagram Protocol.

User Datagram Protocol (UDP)
Protocolo de Internet que proporciona un servicio de datagramas sin conexión y no seguro. Permite que un programa de aplicación situado en una máquina o proceso envíe un datagrama a un programa de aplicación situado en otra máquina o proceso.

V

vulnerabilidad
Riesgo de seguridad en un sistema operativo, software del sistema o componente de software de aplicación.

Índice

I

L

M

N

P

Q

R

S

T

U

V

W

Z

Impreso en España