IBM QRadar Vulnerability Manager
Versión 7.4.0

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 141.

Información sobre el producto

Este documento es aplicable a IBM® QRadar Security Intelligence Platform V7.4.0 y a los releases subsiguientes a menos que sean reemplazados por una versión actualizada de este documento.

Contenido

Visión general de IBM QRadar Vulnerability Manager

Esta información está pensada para ser utilizada con IBM 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 QRadar SIEM o IBM QRadar Log Manager.

Público al que va dirigido este manual

Los administradores del sistema encargados de configurar IBM QRadar Vulnerability Manager debe tener acceso administrativo a IBM 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 V7.4.0

QRadar Vulnerability Manager V7.4.0 incluye un nuevo parámetro de búsqueda para identificar vulnerabilidades conflictivas, además de mejoras sobre las excepciones de vulnerabilidad.

Parámetros de búsqueda de vulnerabilidades conflictivas

QRadar Vulnerability Manager V7.4.0 incluye nuevos parámetros de búsqueda que optimizan los datos de vulnerabilidad recuperados de distintos exploradores. Los parámetros **Encontrado por explorador** y **No encontrado por explorador** ofrecen las ventajas siguientes:

- Reducen la redundancia del conjunto de datos mediante la eliminación de vulnerabilidades duplicadas.
- Mejoran la calidad de los resultados reduciendo los posibles falsos positivos.
- Comparan las vulnerabilidades descubiertas por distintos exploradores, a fin de mejorar las técnicas de exploración e identificar las carencias.

Mejora sobre las excepciones de vulnerabilidad

QRadar Vulnerability Manager V7.4.0 elimina una limitación que permitía a los usuarios crear excepciones para una única instancia de vulnerabilidad en una regla de excepción. Ahora, puede crear reglas que incluyan excepciones para distintas vulnerabilidades.

Para obtener más información, consulte la publicación *IBM QRadar Vulnerability Manager - Guía del usuario*.

Capítulo 2. Instalaciones y despliegues

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

Se accede a IBM® Security QRadar Vulnerability Manager mediante la pestaña Vulnerabilidades:

- 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. Puede adquirir la licencia para QRadar Vulnerability Manager por separado y habilitarla utilizando una clave de licencia.

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

Licencia de QRadar Vulnerability Manager

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*. La licencia de QRadar Vulnerability Manager se aplica y procesa en tiempo real a activos explorados de QRadar Vulnerability Manager que tienen como mínimo una dirección IP. La exploración de QRadar Vulnerability Manager debe estar dentro del tiempo de retención configurado para la dirección IP del activo.

1. En la pestaña **Admin**, pulse **Configuración del perfilador de activos**
2. Busque la fila **Retención de IP de activo (en días)** para editar el valor de retención de IP de activo.
3. Cambie el valor de retención o compruebe que es adecuado para sus necesidades. El valor de retención de IP de activo predeterminado es de 120 días.

Licencias de QRadar Vulnerability Manager y QRadar Risk Manager

IBM QRadar Vulnerability Manager y IBM QRadar Risk Manager se combinan en una oferta y ambos se habilitan mediante una sola licencia base. La oferta combinada proporciona una exploración de red integrada y un flujo de trabajo de gestión de vulnerabilidades. Con la licencia base, tiene derecho a utilizar QRadar Vulnerability Manager para explorar hasta 256 activos. Puede integrar QRadar Risk Manager con hasta 50 orígenes de configuración estándar. Si está autorizado para QRadar Vulnerability Manager o QRadar Risk Manager, está automáticamente autorizado para la bonificación de licencia base para el otro producto. Necesitará licencias adicionales para explorar más de 256 activos o para integrar con más de 50 orígenes de configuración.

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. No puede añadir un procesador de vulnerabilidades al dispositivo de QRadar Flow Processor 1728.

Puede añadir el procesador de vulnerabilidades a los dispositivos de QRadar siguientes: 600, 700, 8099, 8024, 8000, 3124, 8026, 2100, 3199, 3126, 8021 y 3100.

Información de actualizaciones automáticas y vulnerabilidades

Cuando ejecuta la actualización automática, obtiene los metadatos de vulnerabilidad más recientes y las herramientas de exploración que están disponibles. Configure las actualizaciones automáticas a través de una conexión de Internet o desde un servidor fuera de línea local. Normalmente, los metadatos de vulnerabilidad y las herramientas de exploración se actualizan semanalmente.

Como métodos recomendados, asegúrese de ejecutar actualizaciones automáticas después de instalar una actualización de software de QRadar. Ejecute la actualización automática desde la pestaña **Admin** pulsando el icono **Actualización automática**.

Para obtener más información sobre la instalación de actualizaciones automáticas de QRadar, consulte la *Guía de administración de IBM QRadar*.

Conceptos relacionados

Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager

Opciones para trasladar el procesador de vulnerabilidades en el despliegue 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 QRadar SIEM para realizar copias de seguridad y restaurar datos de vulnerabilidad y configuración de IBM 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 *Guía de administración de IBM QRadar*.

Puertos utilizados para la comunicación entre los hosts gestionados de QRadar y QRadar Vulnerability Manager

QRadar Vulnerability Manager utiliza puertos seguros para conectarse a hosts gestionados.

Puertos utilizados para la comunicación

La tabla siguiente describe los puertos que se utilizan para la comunicación segura entre los hosts gestionados de QRadar y QRadar Vulnerability Manager.

Tabla 1. Puertos de comunicación de QRadar Vulnerability Manager

Comunicación	Puerto	Protocolo
QRadar Console al procesador de QRadar Vulnerability Manager	22, 9999, 8989, 8844	TCP
QRadar Console al explorador de QRadar Vulnerability Manager	22	TCP
Procesador de QRadar Vulnerability Manager a QRadar Console	443	TCP
Explorador de QRadar Vulnerability Manager al procesador de QRadar Vulnerability Manager	9999	TCP

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. En el menú de navegación ( ), pulse **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 y la contraseña para el host.
6. Para crear un túnel SSH en el puerto 22, seleccione **Cifrar conexiones de host**.
7. Para habilitar la compresión de cifrado para las comunicaciones con un host, seleccione **Compresión de cifrado**.
8. Para habilitar NAT para un host gestionado, seleccione **Conversión de direcciones de red** y añada la información siguiente:

Tabla 2. Configuración de NAT	
Campo	**Descripción**
Grupo NAT	Si el host gestionado se encuentra en la misma subred que la QRadar Console, seleccione la QRadar Console que está en la red habilitada para NAT. Si el host gestionado no se encuentra en la misma subred que la QRadar Console, seleccione el host gestionado que está en la red habilitada para NAT.
IP pública	El host gestionado utiliza esta dirección IP para comunicarse con otros hosts gestionados en redes diferentes que utilizan NAT.

La red habilitada para NAT debe utilizar NAT estática.

9. Pulse **Añadir**.

   Nota: No cierre la ventana hasta que se complete el proceso para añadir el host.
10. Cierre la ventana **Gestión del sistema y licencias**.
11. En la barra de herramientas del panel **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
12. Pulse **Aceptar**.

Conceptos relacionados

Claves de activación del procesador de vulnerabilidades y del dispositivo explorador

Tareas relacionadas

Verificar que se ha desplegado un procesador de vulnerabilidades

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 el menú de navegación (☰), pulse **Admin**.
2. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
3. Pulse **Habilitar procesador**.
4. Seleccione la consola o host gestionado en la lista **Procesador**.

   Si el procesador reside en el host gestionado, puede seleccionar solamente la consola de QRadar.
5. Pulse **Guardar**.
6. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
7. Pulse **Aceptar**.

   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.**

Conceptos relacionados

Claves de activación del procesador de vulnerabilidades y del dispositivo explorador

Verificar que se ha desplegado un procesador de vulnerabilidades

En IBM 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 el menú de navegación (☰), pulse **Admin**.
3. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
4. 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 el menú de navegación (☰), pulse **Admin**.
3. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
4. Pulse el recuadro de selección **Habilitar procesador** para desmarcarlo.
5. Pulse **Eliminar**.
6. Pulse **Guardar**.
7. Cierre la ventana **Gestión del sistema y licencias**.
8. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
9. 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 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 une explorador de vulnerabilidades a cualquiera de los siguientes hosts gestionados de QRadar: QRadar Console, Event Processor, Flow Processor, Combo Processor, Event Collector, QFlow Collector y Data Node.

Nota: El explorador de vulnerabilidades no se puede añadir a App Host, App Node y QRadar Network Insights.

Ejecute una actualización automática al añadir un explorador u otro host gestionado con prestaciones de exploración. Para obtener más información sobre las actualizaciones automáticas, consulte la *Guía de administración* de *IBM Security QRadar*.

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 IBM 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 IBM 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 IBM 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 el menú de navegación (☰), pulse **Admin**.
2. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Añadir host gestionado**.
3. Escriba la dirección IP del host y la contraseña del dispositivo explorador de host gestionado de QRadar Vulnerability Manager.
4. Pulse **Añadir**.

Debe esperar varios minutos mientras se añade el host gestionado.

5. Cierre la ventana **Gestión del sistema y licencias**.
6. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
7. Pulse **Aceptar**.

Conceptos relacionados

Claves de activación del procesador de vulnerabilidades y del dispositivo explorador

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, procesador de sucesos o nodo de datos.

Antes de empezar

En un despliegue todo en uno, el controlador se utiliza como un explorador incorporado. No puede añadir un dispositivo de explorador aparta a una QRadar Console cuando el procesador QRadar Vulnerability Manager está en la QRadar Console. En un despliegue que no sea todo en uno, se recomienda mover el procesador QRadar Vulnerability Manager a un dispositivo dedicado cuando se exploren más de 50 000 activos.

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 el menú de navegación (☰), pulse **Admin**.
2. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
3. Pulse **Añadir exploradores de vulnerabilidad adicionales**.
4. Pulse el icono **+**.
5. 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.
6. Pulse **Guardar**.
7. Cierre la ventana **Gestión del sistema y licencias**.
8. En la barra de herramientas del panel **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.
9. Pulse **Aceptar**.
10. Consulte la lista **Servidor de exploración** de la página **Configuración de perfil de exploración** para asegurarse de que se añade el explorador.

    Para obtener más información, consulte “Crear un perfil de exploración” en la página 39.

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. Si las actualizaciones automáticas para otros exploradores se ejecutan

antes, entonces las actualizaciones automáticas para todos los exploradores pueden no estar totalmente sincronizadas hasta la siguiente actualización diaria.

Tareas relacionadas

Trasladar el procesador de vulnerabilidades a un host gestionado o consola

Explorar activos de la zona desmilitarizada

En IBM 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.

Información relacionada

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

Configurar la red y activos para exploraciones externas

Para explorar los activos en una red DMZ, debe configurar la red e informar a IBM de los activos que desea explorar.

Acerca de esta tarea

Para explorar activos en una red DMZ, debe llevar a cabo los pasos siguientes:

1. Configure la red.
2. Envíe las especificaciones de red necesarias al equipo de exploración externo.

Configuración de la red para exploraciones externas

Para explorar los activos en una red DMZ, antes tiene que configurar la red para las exploraciones externas.

Procedimiento

1. Asegúrese de que el procesador de QRadar Vulnerability Manager tenga acceso a Internet para permitir la comunicación con el explorador de zona desmilitarizada.

   Nota: Se necesita una dirección IP estática.
2. Asegúrese de que todos los activos conectados mediante el escáner de DMZ tengan acceso a Internet.
3. Configure una regla de cortafuegos saliente para que el puerto 443 permita una conexión al escáner de DMZ.

   Consejo: Las conexiones entrantes no son necesarias.
4. Añada `external-scanner.qradar.ibmcloud.com` a la lista blanca en los sistemas de detección de intrusiones en red para habilitar la transparencia integral de certificados entre el procesador de QRadar Vulnerability Manager y el explorador de zona desmilitarizada.

Envío de las especificaciones de red al equipo de escáner externo

Tras configurar la red para las exploraciones externas, tiene que notificar a IBM los activos que quiere explorar.

Procedimiento

Envíe las siguientes especificaciones de red al equipo de exploración externo a QRadar-QVM-Hosted-Scanner@hursley.ibm.com.

Opción	Descripción
Dirección IP de pasarela	IP externa/pública del procesador QRadar Vulnerability Manager (donde se origina la exploración). Si utiliza un servidor proxy, proporcione la IP del servidor proxy en su lugar.
Equilibradores de carga (opcional)	Si utiliza equilibradores de carga, se necesitará una lista explícita o un rango de todos los equilibradores de carga.
Lista/Rango de direcciones IP	La lista o el rango explícito de todos los activos que se van a explorar.

Restricción: Las exploraciones de DMZ/External no se llevan a cabo de forma satisfactoria hasta que se envía la información solicitada a QRadar-QVM-Hosted-Scanner@hursley.ibm.com y se recibe un correo electrónico de confirmación.

Información relacionada

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

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 el menú de navegación (☰), pulse **Admin**.
2. Haga clic en **Configuración del sistema**.
3. Pulse **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Pulse **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
6. Pulse **Utilizar explorador externo**.
7. 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.
8. Si la red está configurada para utilizar un servidor proxy, pulse **Habilitar servidor proxy** y escriba los detalles del servidor.
9. Pulse **Guardar** y, a continuación, pulse **Cerrar**.
10. En la barra de herramientas del panel **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
11. Pulse **Aceptar**.

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

Información relacionada

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

Navegadores web soportados

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

La tabla siguiente lista las versiones soportadas de navegadores web.

Tabla 3. Navegadores web soportados para productos QRadar	
Navegador web	**Versiones soportadas**
Mozilla Firefox de 64 bits	60 Extended Support Release y posterior
Microsoft Edge de 64 bits	38.14393 y posterior
Google Chrome de 64 bits	Más reciente

El navegador web Microsoft Internet Explorer deja de ser compatible a partir de QRadar V7.4.0.

Excepciones y certificados de seguridad

Si está utilizando el navegador web Mozilla Firefox, debe añadir una excepción a Mozilla Firefox para iniciar una sesión en QRadar SIEM. Para obtener más información, consulte la documentación del navegador web Mozilla Firefox.

Navegación por la aplicación basada en la web

Cuando utilice QRadar, utilice las opciones de navegación existentes en la interfaz de usuario de QRadar en lugar del botón **Atrás** del navegador web.

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

Si utiliza Microsoft Internet Explorer para acceder a productos de IBM 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.

Exploraciones de alta disponibilidad de QRadar Vulnerability Manager

Utilice un despliegue de alta disponibilidad (HA) de QRadar para mantener la planificación de exploración de vulnerabilidad, si el despliegue de QRadar primario falla.

La alta disponibilidad (HA) versión 2 está soportada en QRadar Vulnerability Manager.

Debe utilizar dispositivos idénticos con configuraciones de software idénticas en la configuración de alta disponibilidad (HA). Para obtener información sobre la configuración de un despliegue de alta disponibilidad (HA), consulte la publicación *IBM QRadar High Availability Guide*.

Exploraciones de alta disponibilidad (HA)

Los siguientes dispositivos están soportados en un despliegue de alta disponibilidad (HA) de QRadar Vulnerability Manager:

- Consola
- Dispositivo explorador (610)
- Dispositivo procesador (600)

Notas importantes
Tome nota de la información siguiente cuando despliega exploración de vulnerabilidades de alta disponibilidad (HA):

- Cancele y reinicie cualquier exploración en curso después de una conmutación por anomalía si las exploraciones estaban en curso durante la conmutación por anomalía.
- Si sustituye un dispositivo en su entorno de alta disponibilidad de exploración HA, puede que no aparezca en el despliegue. Debe volver a añadir el dispositivo en el despliegue de HA, y luego desplegar los cambios.
- Utilice dispositivos y configuraciones idénticos en la configuración de alta disponibilidad (HA).
- Las actualizaciones automáticas no se reanudan después de una conmutación por anomalía. Debe ejecutar una actualización automática en una configuración activa no interrumpida.

Ampliación del periodo de licencia temporal de QRadar Vulnerability Manager

De forma predeterminada, cuando se instala IBM 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 el menú de navegación ( ), pulse **Admin**.
2. Pulse el icono **Gestor de vulnerabilidades** en el área **Inténtelo**.
3. 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.

Exploraciones de alta disponibilidad de QRadar Vulnerability Manager

Utilice un despliegue de alta disponibilidad (HA) de QRadar para mantener la planificación de exploración de vulnerabilidad, si el despliegue de QRadar primario falla.

La alta disponibilidad (HA) versión 2 está soportada en QRadar Vulnerability Manager.

Debe utilizar dispositivos idénticos con configuraciones de software idénticas en la configuración de alta disponibilidad (HA). Para obtener información sobre la configuración de un despliegue de alta disponibilidad (HA), consulte la publicación *IBM QRadar High Availability Guide*.

Exploraciones de alta disponibilidad (HA)

Los siguientes dispositivos están soportados en un despliegue de alta disponibilidad (HA) de QRadar Vulnerability Manager:

- Consola
- Dispositivo explorador (610)
- Dispositivo procesador (600)

Notas importantes
Tome nota de la información siguiente cuando despliega exploración de vulnerabilidades de alta disponibilidad (HA):

- Cancele y reinicie cualquier exploración en curso después de una conmutación por anomalía si las exploraciones estaban en curso durante la conmutación por anomalía.

- Si sustituye un dispositivo en su entorno de alta disponibilidad de exploración HA, puede que no aparezca en el despliegue. Debe volver a añadir el dispositivo en el despliegue de HA, y luego desplegar los cambios.
- Utilice dispositivos y configuraciones idénticos en la configuración de alta disponibilidad (HA).
- Las actualizaciones automáticas no se reanudan después de una conmutación por anomalía. Debe ejecutar una actualización automática en una configuración activa no interrumpida.

Capítulo 3. Visión general de QRadar Vulnerability Manager

IBM 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.

Nota: Al desplegar, QRadar Vulnerability Manager actualiza automáticamente el bloque de construcción **BB:Host Definition: VA Scanner Source IP** predeterminado para incluir las ubicaciones de todos los procesadores de QVM. Este comportamiento es intencionado.

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

Exploración de vulnerabilidades

En IBM 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.

Categorías de comprobaciones de vulnerabilidad de QRadar Vulnerability Manager

Comprobaciones de IBM QRadar Vulnerability Manager para varios tipos de vulnerabilidades en la red.

Las vulnerabilidades se clasifican en las siguientes categorías:

- Valores predeterminados arriesgados
- Características de software
- Configuración errónea
- Defectos de proveedor

Valores predeterminados arriesgados

Si deja algunos valores predeterminados, su red puede ser vulnerable a ataques. Las situaciones siguientes son ejemplos que pueden hacer que su red sea vulnerable:

- Dejar páginas o scripts de ejemplo en una instalación de IIS
- No cambiar la contraseña predeterminada en un concentrador/conmutador 3Com
- Dejar "public" o "private" como nombre de comunidad SNMP en un dispositivo habilitado para SNMP
- No establecer la contraseña de inicio de sesión de sa en un servidor MS-SQL

Características de software

Algunos valores de software para sistemas o aplicaciones están diseñados para ayudar en la usabilidad, pero estos valores pueden presentar riesgos para la red. Por ejemplo, el protocolo Microsoft NetBIOS es útil en redes internas, pero si se expone a Internet o un segmento de red no de confianza, presenta riesgos para la red.

Los ejemplos siguientes son mandatos o características de software que pueden presentar un riesgo para la red:

- Solicitudes de máscara de red o indicación de fecha y hora ICMP
- Mandatos para ampliar o verificar Sendmail
- Servicios de protocolo Ident que identifican el propietario de un proceso en ejecución.

Configuración errónea

Además de identificar configuraciones incorrectas en valores predeterminados, QRadar Vulnerability Manager puede identificar una amplia gama de configuraciones incorrectas como, por ejemplo, en los siguientes casos:

- SMTP Relay
- Compartición de archivos NetBios sin restricciones
- Transferencias de zona de DNS
- Directorios grabables FTP World
- Cuentas de administración predeterminadas que no tienen contraseñas
- Directorios exportables NFS World

Defectos de proveedor

Defectos de proveedor es una categoría amplia que incluye sucesos como desbordamientos de almacenamiento intermedio, cuestiones de formato de series, transversales de directorio y script entre sitios. Las vulnerabilidades que requieren un parche o un arreglo de actualización se incluyen en esta categoría.

Comprobaciones realizadas por QRadar Vulnerability Manager

QRadar Vulnerability Manager utiliza una combinación de comprobaciones activas que implica el envío de paquetes y sondeos remotos y comprobaciones de correlación pasivas. La base de datos de QRadar Vulnerability Manager cubre aproximadamente 70.000 vulnerabilidades de capa de aplicación, red y sistema operativo.

Puede hacer búsquedas en la biblioteca de exploración completa por CVE, rango de fechas, nombre del proveedor, nombre de producto, versión del producto y nombre de exposición desde la ventana **Investigar** en la pestaña **Vulnerabilidades**.

Pruebas de QRadar Vulnerability Manager

Los ejemplos siguientes son algunas de las categorías que QRadar Vulnerability Manager prueba:

- Comprobaciones de base de datos
- Comprobaciones de servidor web
- Comprobaciones de servidor de aplicaciones web
- Comprobaciones de scripts web comunes
- Comprobaciones de aplicaciones web personalizadas
- Comprobaciones de servidor DNS
- Comprobaciones de servidor de correo
- Comprobaciones de servidor de aplicaciones
- Comprobaciones de punto de acceso sin cables
- Comprobaciones de servicio común
- Sistemas y software obsoletos

La tabla siguiente describe algunas comprobaciones que realiza QRadar Vulnerability Manager.

Tabla 4. Tipos de comprobaciones de QRadar Vulnerability Manager

Tipo de comprobación	Descripción
Exploración de puertos	Explora en busca de hosts activos y de los puertos y servicios abiertos en cada host activo. Devuelve MAC si el host se encuentra en la misma subred que el explorador. Devuelve información sobre el sistema operativo.

Tabla 4. Tipos de comprobaciones de QRadar Vulnerability Manager (continuación)	
Tipo de comprobación	**Descripción**
Exploración de aplicaciones web	Comprueba cada una de las aplicaciones web y páginas web en un servidor web utilizando las siguientes comprobaciones: Subida de archivo Exploración de directorio HTTP CWE-22 – limitación indebida de un nombre de vía de acceso a un directorio restringido (cruce de vía de acceso) Archivo interesante / visto en registros Completar automáticamente la contraseña en el navegador Configuración incorrecta en archivos predeterminados Divulgación de información Formulario de inicio de sesión no cifrado Directorio indexable: comprueba si los directorios del servidor se pueden examinar HTTP PUT permitido: comprueba si la opción PUT está habilitada en los directorios del servidor Existencia de archivos obsoletos Exploración CGI: comprobaciones de página web común Inyección (XSS/script/HTML) Recuperación de archivos remota (en todos los servidores) Ejecución de mandato desde shell remoto Inyección de SQL, incluyendo ignorar autenticación, identificación de software y origen remoto Opciones de ajuste inverso, excepto para las opciones especificadas. **Nota:** La exploración de aplicaciones web autenticadas no está soportada. Por ejemplo, si es necesaria la autenticación para acceder al sitio, no puede ejecutar pruebas de aplicación web.
SO	Nombre de usuario y divulgación de contraseña Acceso a sistemas de archivos Nombres de usuario y contraseñas predeterminadas Escalamiento de privilegios Denegación de servicio Ejecución de mandatos remota Scripts entre sitios (Microsoft)
Base de datos	Explotaciones y acceso abierto a bases de datos. Contraseñas predeterminadas Nombres de usuario y contraseñas en peligro Denegación de servicio Derechos de administración

Tabla 4. Tipos de comprobaciones de QRadar Vulnerability Manager (continuación)

Tipo de comprobación	**Descripción**
Servidor web	Vulnerabilidades conocidas, explotaciones y problemas de configuración en servidores web. Denegación de servicio Contraseñas de administración predeterminadas Capacidad vista de sistema de archivos Scripts entre sitios
Scripts web comunes	Scripts web que se encuentran normalmente, como CGI Scripts relacionados con el comercio electrónico ASP PHP
Servidor DNS	Cifrado de contraseña débil Denegación de servicio Determinar nombres de cuenta Enviar correos electrónicos Leer correos electrónicos arbitrarios e información confidencial de cuenta Obtener acceso de administración
Punto de acceso inalámbrico	Contraseñas de cuenta de administrador predeterminadas Nombres de comunidad SNMP predeterminados Almacenamiento de contraseña de texto sin formato Denegación de servicio
Servicios comunes	Sistema de nombres de dominio (DNS) Protocolo de transferencia de archivos (FTP) Protocolo simple de transferencia de correo (SMTP)
Servidor de aplicaciones	Ignorar autenticación Denegación de servicio Divulgación de información Nombres de usuario y contraseñas predeterminadas Permisos de archivo débiles Scripts entre sitios
Elipse	Vulnerabilidades del lado del cliente en IE, Chrome, Skype y otros.
Prueba de contraseñas	Prueba predeterminada de contraseñas
Exploración de parches de Windows	Recopila entradas de clave de registro, servicios de Windows, aplicaciones instaladas de Windows y errores de Microsoft con parches.
Exploración de parches de UNIX	Recopila detalles de RPM instalados

Exploración de aplicaciones web

QRadar Vulnerability Manager utiliza la exploración no autenticada para la exploración de aplicaciones web principales. La lista siguiente describe las comprobaciones de vulnerabilidades web de QRadar Vulnerability Manager:

- Vulnerabilidades de inyección de SQL

  Las vulnerabilidades de inyección de SQL se producen cuando programas mal escritos aceptan datos proporcionados por el usuario en una consulta de base de datos sin validar la entrada, que se encuentra en páginas web que tienen contenido dinámico. Mediante pruebas de vulnerabilidades de inyección de SQL, QRadar Vulnerability Manager asegura que existe la autorización necesaria para evitar que se produzcan estas explotaciones.
- Vulnerabilidades de scripts entre sitios (XSS)

  Las vulnerabilidades de scripts entre sitios pueden permitir que los usuarios maliciosos inyecten código en páginas web vistas por otros usuarios. Scripts HTML y del lado del cliente son ejemplos de código que puede inyectarse en páginas web. Los atacantes pueden utilizar la vulnerabilidad de script entre sitios para eludir controles de acceso como, por ejemplo, la política del mismo origen. QRadar Vulnerability Manager prueba varias vulnerabilidades de script entre sitios persistentes y no persistentes para asegurarse de que la aplicación web no es susceptible de esta amenaza.
- Infraestructura de aplicaciones web

  QRadar Vulnerability Manager incluye miles de comprobaciones que comprueban configuraciones predeterminadas, scripts cgi, aplicaciones instaladas y de soporte, sistemas operativos subyacentes y dispositivos.
- Errores de página web

Para una exploración de aplicación web en profundidad, QRadar Vulnerability Manager se integra con IBM Security AppScan para proporcionar mayor visibilidad de aplicación web a sus vulnerabilidades.

Exploración de dispositivo de red

QRadar Vulnerability Manager incluye los siguientes plugin que dan soporte a la exploración de dispositivos de red:

- SNMP

  QRadar Vulnerability Manager es compatible con SNMP V1 y SNMP V2. No se admite SNMP V3. QRadar Vulnerability Manager utiliza un diccionario de valores predeterminados de comunidad conocidos para varios dispositivos habilitados para SNMP. Puede personalizar el diccionario.
- Exploración OVAL

  QRadar Vulnerability Manager utiliza OVAL para detectar e informar de vulnerabilidades conocidas. El plugin de exploración OVAL de QRadar Vulnerability Manager actualmente sólo funciona con dispositivos Cisco.

Comprobaciones de explorador externas

El explorador externo explora las siguientes CWE (Common Weakness Enumerations) de OWASP (Open Web Application Security Project):

- Listado de directorios
- Cruce de vía de accesos, Modificación de parámetros de archivos Windows, Modificación de parámetros de archivos UNIX, Obtención de archivos Poison Null Byte de Windows, Obtención de archivos Poison Null Byte de UNIX
- Script entre sitios, Script entre sitios basado en DOM
- Inyección de SQL, Inyección de SQL ciega, Inyección de SQL ciega (basada en tiempo)
- El atributo HTML Autocomplete no está inhabilitado en el campo Contraseña
- Solicitud de inicio de sesión sin cifrar, Parámetro de contraseña sin cifrar

- Ejecución remota de código, Inyección de código de llamada al sistema, Inyección de mandato de shell de parámetro de archivo, Ejecución de mandato remota de serie de formato

Exploración de bases de datos

QRadar Vulnerability Manager detecta vulnerabilidades en bases de datos grandes utilizando la exploración autenticada de hosts de destino. Además, QRadar Vulnerability Manager se dirige a varias bases de datos utilizando plugins.

Comprobaciones de sistema operativo

Tabla 5. Comprobaciones de sistema operativo

Sistema operativo	Exploración de vulnerabilidades	Exploración de parches	Configuración
Windows	Sí	Sí	Sí
AIX UNIX	Sí	Sí	No
CentOS Linux	Sí	Sí	No
Debian Linux	Sí	Sí	No
Fedora Linux	Sí	Sí	No
Red Hat Linux	Sí	Sí	No
Sun Solaris	Sí	Sí	No
HP-UX	Sí	Sí	No
Suse Linux	Sí	Sí	No
Ubuntu Linux	Sí	Sí	No
CISCO	No	No	No
AS/400 / iSeries	No	No	No

OVALs y sistemas operativos

Las definiciones de OVAL están soportadas en los siguientes sistemas operativos:

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- CentOS versiones 3 – 7
- IBM AIX versiones 4-7
- RHEL versiones 3 – 7
- SUSE versiones 10 – 11

- Ubuntu versiones 6-14
- Red Hat 9
- Solaris versiones 2.6, 7 - 10

Panel de control de gestión de vulnerabilidades

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

IBM 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. 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**.

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. Estrategia de exploración de vulnerabilidades y mejores prácticas

Una buena planificación es esencial para la configuración de un sistema de exploración de IBM QRadar Vulnerability Manager estable y eficiente en la red.

Analice la estructura de red y determine la mejor configuración de exploración de la red, tanto desde la perspectiva del hardware como desde la perspectiva del rendimiento de la exploración.

Tenga en cuenta la siguiente información, que incluye las mejores prácticas para configurar el despliegue de la exploración de QRadar Vulnerability Manager:

- Tipos de política de exploración

  Elija el tipo de política de exploración que satisfaga sus necesidades de exploración y tenga en cuenta el tiempo y los recursos que se necesitan para completar la exploración.
- Duración de la exploración y puertos a explorar

  Decida si es necesario explorar todos los puertos TCP y UDP. Los puertos UDP tardan más tiempo en explorarse que los puertos TCP.
- Ajustar el descubrimiento de activos

  Ajuste el descubrimiento de activos para gestionar los tiempos de descubrimiento de activo y la efectividad.
- Ajustar el rendimiento del descubrimiento de activos.

  Ajuste y optimice la velocidad y precisión con la que se descubren activos en la red.
- Situación del explorador en la red

  Sitúe los exploradores cerca de los activos que está explorando, y sea consciente del impacto de la latencia de red sobre los tiempos de exploración.
- Exploración de aplicaciones web

  Esta exploración puede tardar mucho tiempo y utilizar recursos de forma intensiva. Si no necesita ejecutar esta exploración como parte de una exploración completa, puede excluirla.
- Exploración dinámica

  Puede ahorrar tiempo implementando la exploración dinámica.
- Valores de ancho de banda de red

  Ajuste el valor de ancho de banda de red de acuerdo con su ancho de banda de red y el número de activos que puede explorar simultáneamente.
- Tarjetas de interfaz de red en exploradores

  Utilice tarjetas de interfaz de red para segmentar la exploración de red.
- Gestión de vulnerabilidades para propietarios de activo

  Asigne propietarios a los activos.
- Notificación a propietarios de activos sobre los tiempos de las exploraciones.

  Asegúrese de que los propietarios de activos tienen conocimiento de los tiempos de exploración.
- Desencadenamiento de exploraciones de activos nuevos

  Desencadenar exploraciones de activos nuevos cuando se añaden a la base de datos de activos.
- Configurar riesgos medioambientales para un activo

  Utilice la Puntuación ambiental CVSS para manipular y priorizar la puntuación de riesgo en activos seleccionados.

- Preguntas más frecuentes sobre exploración externa

  Lo que debe saber sobre la configuración de una exploración externa.

Tipos de política de exploración

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

A continuación se indican las plantillas de exploración utilizadas con más frecuencia:

Política de exploración de descubrimiento

Descubre activos de red y luego explora los puertos para identificar las características de activos clave, como por ejemplo sistema operativo, tipo de dispositivo y los servicios. Las vulnerabilidades no se exploran.

Es una exploración ligera sin credenciales que busca en un espacio de direcciones las direcciones IP activas y, a continuación, explora sus puertos. Ejecuta búsquedas DNS y NetBIOS para descubrir el sistema operativo, servicios abiertos y nombres de red.

Si es posible, ejecute esta exploración sin credenciales semanalmente para ofrecer una buena visibilidad de la red. Esta exploración es útil principalmente para identificar nuevos activos y cambios de activos explorados anteriormente.

Nota: Utilice la búsqueda guardada **activos vistos en los últimos 14 días pero no explorados** de la pestaña **Activos** para identificar nuevos activos que QRadar descubrió pasivamente en los últimos 14 días.

Política de exploración completa

Descubre los activos de la red mediante un rango de puertos de exploración rápida. Ejecuta 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. Se ejecuta una exploración autenticada cuando se proporcionan credenciales.

Ejecuta la suite completa de pruebas de QRadar Vulnerability Manager.

Una exploración completa tiene estas fases:

1. Exploración de descubrimiento.
2. Exploración 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. Exploración con credenciales.

   QRadar Vulnerability Manager inicia sesión en el activo y recopila información acerca del inventario de aplicaciones instaladas y la configuración necesaria; también genera o suprime vulnerabilidades. Las exploraciones con 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 exhaustivo y eficaz.

   No puede editar las políticas incorporadas pero puede copiarlas para crear sus propia política de exploración personalizada.

   Consejo: las exploraciones completas a veces pueden bloquear algunas cuentas de administración (por ejemplo, SQL Server) cuando QRadar Vulnerability Manager prueba varias credenciales predeterminadas en las cuentas. Desactive estas pruebas de inicio de sesión realizando los pasos siguientes:

   a. Pulse la pestaña **Vulnerabilidades**.

   b. En la ventana **Política de exploración**, pulse **Políticas de exploración**.

c. Pulse la política **Exploración completa** y, a continuación, pulse **Editar**.

d. Pulse la pestaña **Herramientas**.

De forma predeterminada, se visualiza la lista **Incluido**.

e. En el menú **Filtro**, seleccione **Inicios de sesión predeterminados (Riesgo de denegación de servicio)**.

f. Pulse **Excluir todo** para eliminar las marcas de comprobación junto a los elementos de la lista.

g. Pulse **Guardar**.

h. Verifique que las herramientas **Inicios de sesión predeterminados (Riesgo de denegación de servicio)** están en la lista **Excluido**.

Ejecute una exploración completa cada 2-3 meses para realizar una evaluación detallada y precisa de las vulnerabilidades de la red. La exploración completa consume recursos de forma intensiva, por lo que la planificación y la asignación de recursos es importante para obtener un rendimiento óptimo.

Política de exploración de parches

Explora la red para descubrir activos y después ejecuta una exploración rápida de puertos y una exploración con credenciales de los activos.

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:

1. Exploración de descubrimiento
2. Exploración con credenciales

Ejecute esta exploración con credenciales cada 1-4 semanas para determinar qué parches y productos están instalados o faltan en la red. La exploración de parches implica sólo una mínima carga en la red y las pruebas activas se mantienen en un nivel bajo.

Política de exploración de PCI

Explora todos los puertos TCP y UDP 0-65535.

No es necesario explorar todos los puertos de UDP para la conformidad con PCI. Normalmente puede explorar los puertos de UDP más comunes para la conformidad con PCI pero la lista de puertos puede cambiar ligeramente a lo largo del tiempo de acuerdo con los estándares de seguridad de PCI.

Si explora todos los puertos de UDP, la exploración puede tardar mucho tiempo y no completarse dentro del periodo en grandes segmentos de red, lo que provoca algunas instancias de vulnerabilidad `Interferencia de exploración detectada - Exploración posiblemente incompleta`.

Puede crear su propia política de exploración de PCI copiando esta política, redenominando la política y modificando los puertos de exploración de UDP según sus requisitos.

Política de exploración de base de datos

Explora los puertos de base de datos 523, 1433, 1521 y 3306 con respecto a servicios de base de datos habituales.

Utilice la exploración de bases de datos sin credenciales para explorar los puertos DB2 (523), Microsoft SQL (1433), MySQL (3306), Oracle (1521) e Informix (1526) para servicios de base de datos habituales.

Ejecute esta exploración regularmente si tiene una actividad de base de datos elevada.

Conceptos relacionados

Políticas de exploración

Duración de la exploración y exploración de puertos

La gestión de la configuración de exploración de red está influenciada por el número de activos de la red, la infraestructura de red y los tiempos de finalización de la exploración.

Puede tardar mucho tiempo en explorar una red de grandes dimensiones, por lo que necesita una estrategia de exploración que optimice sus recursos de exploración.

Consejo: Siempre es recomendable utilizar ventanas operativas para realizar exploraciones en momentos en los que no se solapan con actualizaciones automáticas o copias de seguridad nocturnas.

Estrategia de exploración de puertos

La estrategia de exploración está influenciada por el número de hosts que desea explorar, ya sea una red de clase C de 256 hosts o una red de clase B de 65.536 hosts. El tiempo de exploración global puede resultar significativamente afectado por el aumento del número de hosts que desee explorar. Para situar el tiempo de exploración global en un rango aceptable, puede reducir el tiempo de exploración por host.

Por ejemplo, si realiza una exploración de descubrimiento de red en una red de clase B que tarda 1 segundo para el descubrimiento de puertos TCP, las afirmaciones siguientes son verdaderas:

- La exploración de un puerto en 65536 hosts a 1 segundo por host tarda 18 horas.
- Si explora un puerto adicional en cada uno de los 65536 hosts y permite 1 segundo por host, tardará otras 18 horas en explorar ese puerto adicional.

En el ejemplo, puede ver el impacto de añadir un puerto de exploración adicional en una red de grandes dimensiones. Si está explorando un gran número de hosts, debe comprender qué servicios son importantes y son propensos a vulnerabilidades de alto riesgo para poder configurar adecuadamente las políticas de exploración en la etapa de exploración de descubrimiento. Antes de implementar sus políticas de exploración, ejecute exploraciones de prueba utilizando diferentes políticas de exploración y calcule el tiempo y los recursos que son necesarios para realizarlas.

Consejo: La política de exploración de descubrimiento predeterminada de QRadar ejecuta una exploración rápida Nmap de puertos TCP y UDP, y puede utilizarla para explorar un número más reducido de hosts.

La exploración de puertos UDP tarda más tiempo que la exploración de puertos TCP porque es un protocolo sin conexión. La exploración de todos los puertos UDP puede tardar mucho tiempo y utiliza recursos de forma intensiva. Considere si es necesario explorar todos los puertos UDP o si puede explorar estos puertos con menos frecuencia que los puertos TCP.

Los siguientes puertos son algunos de los puertos UDP de prioridad más alta que debe considerar explorar periódicamente:

- Servicios de autenticación como RADIUS y Kerberos
- Aplicaciones de acceso remoto y puertas traseras
- Aplicaciones de copia de seguridad
- Servidores de bases de datos
- DNS (Sistema de nombres de dominio)
- NetBIOS y Common Internet File System (CIFS)
- NFS (Network File System)
- NTP (Network Time Protocol)
- P2P (igual a igual) y aplicaciones de chat
- Protocolos de direccionamiento, incluyendo RIP (protocolo de información de direccionamiento)
- RPC (llamada a procedimiento remoto) y correlación de punto final RPC
- SNMP (Simple Network Management Protocol) y condición de excepción SNMP
- Syslog

- TFTP (Trivial File Transfer Protocol)
- VPNs, incluidos Internet Security Association and Key Management Protocol (ISAKMP), Layer Two Tunneling Protocol (L2TP) y (NAT Traversal) NAT-T.
- Puertos que están asociados con actividad maliciosa.

Tiempos de exploración típicos

La tabla siguiente proporciona información sobre los tiempos de exploración.

Tabla 6. Tiempos de exploración para dispositivos de QRadar

Dispositivo QRadar	**Tiempos de exploración**
QRadar 2100/3100 All-in-One	Una exploración completa predeterminada de 2000-4000 activos tarda 2-3 días.
QRadar Vulnerability Manageren los hosts gestionados siguientes: 610 1200 1300 1400 1500	Una exploración completa predeterminada de 2000-4000 activos tarda 2-3 días. Es necesario un procesador de QRadar Vulnerability Manager externo en un host gestionado (600) si se exploran regularmente más de 50.000 activos o si se ejecutan exploraciones durante largos períodos de tiempo en QRadar Console.

Ajustar la configuración de descubrimiento de activos

Ajuste el descubrimiento de activos para gestionar los tiempos de descubrimiento de activo y la efectividad.

Ajuste el descubrimiento de activos de la pestaña **Asset Discovery** de la política de exploración. Puede utilizar la configuración predeterminada como una forma rápida y eficiente de descubrir los activos. Los pings de ICMP y los paquetes de TCP SYN están habilitados de forma predeterminada.

Utilice las opciones siguientes para ajustar el descubrimiento de activos:

- Enviar pings ICMP.

  Los pings se envían a las direcciones IP configuradas en el perfil de exploración que utiliza esta política de exploración.
- Enviar paquetes TCP SYN a puertos.

  Esta opción es una opción rápida fiable habilitada para puertos preconfigurados.
- Enviar paquetes UDP a puertos.

  Seleccione esta opción para enviar paquetes UDP a puertos preconfigurados. UDP es más lento que TCP. Si envía un paquete UDP a una dirección IP inactiva, tardará varios segundos en completarse debido a los reintentos.
- Habilitar detección de traceroute.

  La detección de traceroute necesita más recursos y los tiempos de exploración aumentan.
- Habilitar detección de ICMP.

  La detección de ICMP necesita más recursos y los tiempos de exploración aumentan.
- Huellas digitales de sistema operativo y de servicio

  Sondear puertos en busca información de sistema operativo y de servicio. Si selecciona esta opción, los tiempos de exploración aumentan.

Puede configurar opciones de descubrimiento personalizadas. Las opciones que elige dependen de los requisitos y la estructura de red. Pruebe varias opciones para descubrir una configuración de descubrimiento óptima que coincida con sus necesidades.

Ajustar el rendimiento del descubrimiento de activos

Ajuste y optimice la velocidad y precisión con la que se descubren servicios en los activos.

Ajuste el rendimiento de descubrimiento en la pestaña **Rendimiento de descubrimiento** de la política de exploración. Puede utilizar la configuración predeterminada como una forma rápida y eficiente de descubrir los activos.

Utilice las opciones siguientes para ajustar el rendimiento del descubrimiento de activos:

- **Número máximo de reintentos**

  Los tiempos de exploración pueden aumentar cuando se aumenta el número máximo de reintentos, pero cuando se establece este número demasiado bajo, la precisión de los resultados de exploración puede verse afectada.

- **Intervalo de tiempo de espera mínimo**

  El intervalo de tiempo de espera de exploración se reduce al nivel mínimo configurado cuando la red es fiable.

- **Intervalo de tiempo de espera inicial**

  Nmap ajusta el valor de tiempo de espera en respuesta a análisis anteriores. Si aumenta la latencia, el valor de tiempo de espera se incrementa. Si disminuye tanto el tiempo de espera inicial como los intervalos de tiempo de espera máximo a valores demasiado bajos, los tiempos de exploración pueden ser más rápidos, pero hay el riesgo de tener que retransmitir.

- **Retardo de exploración**

  Utilice este valor para ajustar el retraso entre sondeos de exploración. Si los dispositivos utilizan limitación de velocidad, puede sincronizar el retardo de exploración con el valor de límite de velocidad para conseguir los tiempos de exploración óptimos.

- **Mínimo de paquetes por segundo**

  Nmap envía paquetes a la velocidad más alta posible que tolera la red, entre la velocidad **Mínimo de paquetes por segundo** y la velocidad **Máximo de paquetes por segundo**.

- **Máximo de paquetes por segundo**

  De forma predeterminada, este campo está vacío porque Nmap establece dinámicamente una velocidad de paquetes adecuada para su red. Si lo desea, puede configurar su propia velocidad.

Exploración de aplicaciones web

Las exploraciones web pueden ser lentas si tiene aplicaciones web complejas. Se exploran todos los puertos que ejecutan servicios HTTP o HTTPS, incluidos los puertos de Microsoft HTTP RPC.

Parte de una exploración completa o una exploración web incluye una fase que utiliza técnicas de uso intensivo de recursos que es similar al rastreo web o al recorrido e indexación (spidering). Si el explorador debe rastrear varias páginas web que tienen varios enlaces, la exploración puede ser lenta y exigente en cuanto a los recursos. Las exploraciones web buscan vulnerabilidades web, como por ejemplo determinar si una versión del servidor HTTP tiene vulnerabilidades, certificados SSL caducados o cifrados SSL débiles. La exploración web también busca vulnerabilidades OWASP (Open Web Application Security Project), como por ejemplo inyección SQL, script entre sitios (XSS), configuraciones de seguridad incorrectas.

Si no es necesario explorar las aplicaciones web, cree una política de exploración completa personalizada y excluya la herramienta de exploración **http - CGI scanner** que está en la pestaña **Herramientas** de la política de exploración.

Situación del explorador en la red

Las operaciones de exploración son más eficientes cuando los exploradores tienen una buena conectividad con los activos que se exploran y no están obstaculizadas por cortafuegos o otros dispositivos que afecten al flujo de los datos de exploración. Puede desplegar un número ilimitado de exploradores en la red, pero debe tener una licencia de software para cada host gestionado de QRadar que despliegue como explorador.

Tenga en cuenta los factores siguientes antes de situar exploradores en la red:

- Evite la exploración de activos a través de cortafuegos por las siguientes razones:
  - Los cortafuegos ralentizan la exploración y bloquean algunos puertos que son necesarios para realizarla.
  - Cuando se exploran activos a través de un cortafuegos, se crean sucesos en IBM QRadar y aumentan los números de EPS (sucesos por segundo), lo que puede afectar a su licencia de EPS.
  - Los cortafuegos con estado pueden provocar que QRadar cree activos erróneamente. Los cortafuegos con estado responden a paquetes TCP desfasados, y eso puede hacer que el explorador crea que un host existe.
- No explore a través de conexiones WAN de bajo ancho de banda.
- Si el tiempo de ping del explorador al activo es de 40 ms, sitúe el explorador más cerca del activo.
- No explore a través de un equilibrador de carga porque es más difícil para el explorador gestionar la exploración cuando la carga del tráfico de red se equilibra entre servidores diferentes.
- Evite configurar el explorador para explorar rangos de direcciones IP que sabe que no se utilizan. Durante la fase de descubrimiento de una exploración, un explorador tarda más tiempo en determinar que una dirección IP no se está utilizando que el que emplea para determinar si una dirección IP está activa.
- Despliegue más exploradores en lugar de ejecutar varias exploraciones simultáneas desde el mismo explorador. A medida que se añaden más exploraciones simultáneas al mismo explorador, los recursos se reducen y cada exploración tarda mucho más.

Exploración dinámica

Utilice la exploración dinámica en IBM QRadar Vulnerability Manager para asociar exploradores individuales con una dirección IP, rangos de CIDR, rangos de direcciones IP o un dominio que especifique en el perfil de exploración. La exploración dinámica es más útil cuando se despliegan varios exploradores. Por ejemplo, si despliega más de 5 exploradores, puede ahorrar tiempo utilizando la exploración dinámica.

Las ventajas de implementar la exploración dinámica dependen de la infraestructura de red y del número de exploradores que están disponibles. Por ejemplo, si tiene diez exploradores de QRadar Vulnerability Manager y no utiliza la exploración dinámica, debe configurar diez trabajos de exploración individuales. QRadar Vulnerability Manager selecciona el explorador apropiado para cada dirección IP que se va a explorar.

Si se utiliza la exploración dinámica en el perfil de exploración y asocia 2 exploradores con un activo, el explorador que incluye el activo en la subred coincidente más pequeña tiene prioridad para explorar el activo en primer lugar.

Por ejemplo, la dirección IP del activo es 10.2.2.3, y se asigna el explorador A al rango de direcciones CIDR 10.2.2.0/24, y el explorador B a la dirección CIDR 10.2.2.3/32. El explorador B tiene prioridad para explorar el activo antes que el explorador A porque la subred (/32) es una coincidencia exacta para el activo.

Antes de habilitar la exploración dinámica, ejecute exploraciones de prueba y luego evalúe el impacto en los recursos de red, el rendimiento de la exploración y los tiempos de exploración.

Tareas relacionadas

Crear un perfil de exploración

Ancho de banda de red para exploraciones de activos simultáneas

Ajustando el valor de ancho de banda de red, cambiará el número de activos que se pueden explorar simultáneamente y el número de herramientas de vulnerabilidad que pueden utilizarse simultáneamente para explorar los activos. Algunas exploraciones utilizan más herramientas de vulnerabilidad para la exploración, lo cual afecta al número de activos que se pueden explorar simultáneamente.

El valor de ancho de banda de red va de un valor bajo de 200 Kbps a un valor completo de 5000 Kbps. Configure el valor de ancho desde la pestaña de detalles de un perfil de exploración. El valor predeterminado de ancho de banda de red es medio, que es de 1000 Kbps.

Ajuste el ancho de banda según los escenarios siguientes:

- Ajuste el ancho de banda de red a 5000 Kbps (completo) para exploración de parches de hasta 50 activos simultáneamente o manténgalo en 1000 Kbps (medio) para la exploración de parches de 10 activos simultáneamente como máximo.
- Utilice el valor de 5000 Kbps (completo) si la red tiene un buen ancho de banda.
- No utilice el valor de 5000 Kbps a través de una conexión WAN lenta.
- Si explora a través de un cortafuegos y es un origen de registro, el tráfico de exploración crea sucesos, y es posible que tenga que reducir el ancho de banda de red para evitar superar el umbral de licencia de EPS (sucesos por segundo).

Tareas relacionadas

Crear un perfil de exploración

Tarjetas de interfaz de red en exploradores

En IBM 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 4-5. 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.

Si los activos de destino que se están explorando se encuentran en redes diferentes, configure NIC individuales para conectarse a las diversas redes.

Esta segmentación de las redes mediante NIC hace posible que el explorador se conecte directamente a redes diferentes. Por ejemplo, una interfaz Ethernet puede configurarse para conectarse a la red 10.100.85.0/24 y una segunda interfaz de Ethernet puede configurarse para conectarse a la red 192.168.0.0/24.

Gestión de vulnerabilidades para propietarios de activo

Asigne propietarios a los activos para que las vulnerabilidades descubiertas están asignadas a los propietarios de activos. Las vulnerabilidades asignadas se asignan con una fecha de vencimiento, que se calcula en función del nivel de riesgo de la vulnerabilidad.

Configure los informes de remediación que desea enviar a los propietarios de activos resaltando la información siguiente:

- Los parches que deben instalar.
- Los pasos necesarios 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.

Desde la pestaña **Informes** puede crear un informe de vulnerabilidades y asignar este informe a un grupo de informes de exploración. Puede configurar los destinatarios de este informe en un perfil de exploración, que puede verse en la ventana **Informes disponibles** de la pestaña **Qué enviar por correo electrónico** de la pantalla **Configuración de perfil de exploración**.

Utilice 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, utilice QRadar Vulnerability Manager para crear automáticamente vulnerabilidades de activos e informes de 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 configuren explícitamente de otro modo. Todas las vulnerabilidades que se hayan arreglado anteriormente y que se vuelvan a detectar se reabren automáticamente.

Tareas relacionadas

Asignar un usuario técnico como propietario de grupos de activos

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.

Buscar datos de vulnerabilidad

Notificaciones de exploración de vulnerabilidades

Para evitar falsas alarmas cuando la actividad de exploración es elevada, informe a los propietarios de activos de la temporización de las exploraciones.

Algunas herramientas de exploración de QRadar Vulnerability Manager, como por ejemplo las herramientas web, pueden generar una gran cantidad de tráfico. Por ejemplo, una exploración web puede enviar 500 solicitudes HTTP por segundo a servidores HTTP. Si los propietarios de activos ven una cantidad de tráfico inusual, podrían pensar que el activo que se está explorando está sujeto a un ataque de denegación de servicio o a ataques similares.

Configure perfiles de exploración para enviar correos electrónicos a los propietarios de activos y a otras partes interesadas antes y después de una exploración para que sean conscientes de que una cantidad de tráfico de red o de carga superior a la habitual podría producirse en su red. Otra forma de que los propietarios de activos conozcan los tiempos de exploración de activos es acordar con ellos una planificación de exploración.

Configure la notificación de correo electrónico desde la pestaña **Correo electrónico** del perfil de exploración.

Desencadenamiento de exploraciones de activos nuevos

Utilice los sucesos procesados por el motor de reglas personalizadas (CRE) para desencadenar exploraciones sobre activos nuevos cuando se les asignan direcciones IP nuevas.

Antes de empezar

Cree un perfil de exploración con **Exploración a petición** habilitada.

Procedimiento

1. En la pestaña **Actividad de registro**, pulse **Reglas** > **Reglas**.
   También puede acceder al menú de reglas desde las pestañas **Delitos** y **Actividad de red**.
2. En el menú **Acciones**, pulse **Nueva regla de sucesos**.
3. Pulse **Sucesos** y a continuación pulse **Siguiente** para continuar.
4. Añada pruebas a la lista de reglas.
   a) Pulse el icono de adición (**+**) junto a la prueba **cuando los sucesos los han detectado uno o varios de estos orígenes de registro**.
   b) Pulse el icono de adición (**+**) junto a la prueba **cuando el suceso QID es uno de los siguientes QIDs**.
   c) Pulse el icono de adición (**+**) junto a la prueba **y cuando el IP de origen es una de las direcciones IP siguientes**.
5. En el panel **Regla**, edite cada valor de regla.
   a) Para la primera regla, pulse **estos orígenes de registro** y añada el elemento Perfilador de activos de la lista.
   b) Para la segunda regla, pulse **QIDs** y a continuación busque QIDs descritos en la tabla siguiente y añádalos a su regla.

   Tabla 7. Nombres y descripciones de QID para añadir a la regla

QID	Nombre	Descripción
68750030	**Dirección IP creada**	Este suceso se produce cuando se crea un registro de dirección IP nuevo para un activo.
68750013	**Activo creado**	Este suceso se produce cuando se crea un activo nuevo.

   c) Para la tercera regla, pulse **y** para que cambie a **y NO** y a continuación pulse **Direcciones IP** y añada 127.0.0.1

   El ejemplo siguiente es la salida de esta configuración de regla:

   y NO cuando la IP de origen es una de las siguientes 127.0.0.1
6. En el cuadro de texto **Aplicar**, teclee un nombre exclusivo para esta regla, deje **Local** como el valor del sistema predeterminado y pulse **Siguiente**.
7. En la sección **Respuesta de regla**, pulse **Desencadenar exploración**.
   a) En el menú **Perfil de exploración a utilizar como plantilla**, seleccione el perfil de exploración que desea utilizar.

   Debe seleccionar la opción **Exploración a petición** en el perfil de exploración que desea utilizar con esta regla.
   b) Pulse **Origen** para la opción **IPs locales a explorar**.
   c) Especifique valores para el valor **Limitador de respuestas**.

   Configure intervalos adecuados para evitar una posible sobrecarga del sistema.
   d) Si no desea empezar a observar sucesos inmediatamente, quite la marca de la opción **Habilitar regla** y a continuación pulse **Finalizar**.

Configuración de riesgos medioambientales para un activo

Utilice la Puntuación ambiental CVSS para manipular y priorizar la puntuación de riesgo en activos seleccionados. Si configura los parámetros **CVSS, peso y conformidad** para un activo, puede aplicar puntuaciones de riesgo más altas a los activos que son más importantes o críticos.

Acerca de esta tarea

Si tiene activos importantes o críticos y activos menos importantes con las mismas vulnerabilidades, puede configurar la puntuación ambiental CVSS en activos importantes o activos críticos para tener una puntuación de riesgo superior a la de los activos menos importantes. Al aplicar una puntuación de riesgo superior a los activos más importantes, resalta estos activos importantes en los resultados de exploración.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Haga doble clic en el activo que desea editar y, a continuación, pulse **Editar activo**.
4. Pulse **CVSS, peso y conformidad** en la ventana **Editar Perfil**.
5. Configure los parámetros en el panel **CVSS, peso y conformidad**.

   En la tabla siguiente se enumeran los parámetros del panel **CVSS, peso y conformidad**.

Parámetro	Descripción
Potencial de daños colaterales	El potencial de pérdida de vidas humanas o activos físicos a través de daños o el robo de este activo, o la pérdida económica de productividad o ingresos. Si eleva el **Potencial de daños colaterales**, por ejemplo, de **Bajo** a **Alto**, el valor calculado para la **Puntuación CVSS** aumenta. El parámetro **Potencial de daños colaterales** está directamente relacionado con el parámetro **Peso**. Cambiar un parámetro afecta al otro parámetro.
Requisito de confidencialidad	El impacto en confidencialidad para este activo cuando se explota una vulnerabilidad. Si eleva el requisito de confidencialidad, por ejemplo, de **Bajo** a **Alto**, el valor calculado para la **Puntuación CVSS** aumenta.
Requisito de disponibilidad	El impacto en la disponibilidad del activo cuando una vulnerabilidad se explota con éxito. Los ataques que consumen ancho de banda de red, ciclos de procesador o espacio de disco impactan la disponibilidad de un activo. Si eleva el valor del requisito de disponibilidad, por ejemplo, de **Bajo** a **Alto**, el valor calculado para la **Puntuación CVSS** aumenta.
Requisito de integridad	El impacto en la integridad del activo cuando una vulnerabilidad se explota con éxito. La integridad hace referencia a la fiabilidad y la veracidad garantizada de la información. Si eleva el requisito de integridad, por ejemplo, de **Bajo** a **Alto**, el valor calculado para la **Puntuación CVSS** aumenta.
Peso	El **Peso** está enlazado con el valor de **Potencial de daños colaterales**. Si selecciona 10 para el parámetro **Peso**, el **Potencial de daños colaterales** cambia a **Alto**.

6. Pulse **Guardar**.

Preguntas más frecuentes sobre exploración externa

Explore los activos de su zona desmilitarizada (DMZ) o perímetro de red desde la nube mediante un explorador externo alojado por IBM. Ejecute exploraciones sin credenciales desde fuera de la red para proporcionar una defensa añadida a la protección de sus activos de un ataque externo.

¿Qué información necesita proporcionar?

Debe enviar un correo electrónico a QRadar-QVM-Hosted-Scanner@hursley.ibm.com con la información siguiente:

- La dirección IP externa de su empresa.
- Si utiliza equilibradores de carga, debe proporcionar las direcciones IP que utilizan.
- El rango de direcciones IP de los activos contenidos en la zona desmilitarizada.

Nota: Debe tener una instalación local de QRadar Vulnerability Manager.

¿El equipo de QRadar verifica el rango de CIDR proporcionado?

Antes de empezar la exploración, se comprueba el rango de CIDR y se verifica la propiedad.

¿Cuál es el impacto de la exploración externa sobre los servidores como por ejemplo lo servidores web?

La exploración no es intrusiva pero carga los sistemas. Ejecute la exploración cuando los servidores no estén muy activos.

¿Cómo se envían los resultados de exploración desde la nube al procesador de QRadar Vulnerability Manager?

El explorador externo envía los resultados de exploración de la nube al procesador de QRadar Vulnerability Manager a través de una conexión segura.

¿Cuál es el rol de App Scan en el explorador externo?

App Scan explora vulnerabilidades de script entre sitios (XSS) y (Open Web Application Security Project) OWASP en servidores web. Debe proporcionar los nombres de cualesquiera dominios virtuales.

¿Es necesario utilizar un explorador interno para explorar la zona desmilitarizada (DMZ) además del explorador externo?
La mayoría de ataques de red vienen de fuera por lo que explorador externo se dirige a las superficies de ataque externas desde la perspectiva de alguien externo.

Es recomendable ejecutar la exploración externa y una exploración autenticada internamente en en la zona desmilitarizada (DMZ) porque los cortafuegos pueden restringir el acceso a ciertas vulnerabilidades, puertos, servicios y hosts.

Si utiliza un equilibrador de carga para tráfico entrante, es posible que el explorador externo tenga acceso a uno sólo de los servidores que están conectados al equilibrador de carga. En este caso, es posible que daba configurar una ruta de acceso para que el explorador externo pueda explorar todos los servidores. También puede utilizar un explorador externo para explorar estos servidores en la zona desmilitarizada (DMZ).

Capítulo 5. Configuración de la exploración

En IBM 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

Crear un perfil de exploración

En IBM 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 *Guía de administración de IBM QRadar*.

4. Pulse **Guardar**.

Conceptos relacionados

Ancho de banda de red para exploraciones de activos simultáneas
Ajustando el valor de ancho de banda de red, cambiará el número de activos que se pueden explorar simultáneamente y el número de herramientas de vulnerabilidad que pueden utilizarse simultáneamente para explorar los activos. Algunas exploraciones utilizan más herramientas de vulnerabilidad para la exploración, lo cual afecta al número de activos que se pueden explorar simultáneamente.

Exploración dinámica
Utilice la exploración dinámica en IBM QRadar Vulnerability Manager para asociar exploradores individuales con una dirección IP, rangos de CIDR, rangos de direcciones IP o un dominio que especifique en el perfil de exploración. La exploración dinámica es más útil cuando se despliegan varios exploradores. Por ejemplo, si despliega más de 5 exploradores, puede ahorrar tiempo utilizando la exploración dinámica.

Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager

Políticas de exploración

Exploraciones de vulnerabilidades dinámicas
En IBM 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 IBM 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

Configuración de una política de exploración
En IBM QRadar Vulnerability Manager,puede configurar una política de exploración para ajustarse a los requisitos específicos de sus exploraciones de vulnerabilidad. Puede copiar y renombrar una política de exploración preconfigurada o puede añadir una política de exploración nueva. No puede editar una política de exploración preconfigurada.

Crear un perfil de exploración de explorador externo

En IBM 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 11.

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

Ejecución manual de perfiles de exploración

En IBM 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 44.

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 8.

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

Tareas relacionadas

Gestionar resultados de exploración

Reexploración de un activo mediante la opción del menú contextual

En IBM 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

Detalles de perfil de exploración

En IBM 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 8. 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 53.

Conceptos relacionados

Exploraciones de vulnerabilidades dinámicas

En IBM 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

Tareas relacionadas

Creación de un perfil de exploración bajo demanda

Para desencadenar una exploración en respuesta a un suceso de reglas personalizadas, configure un perfil de exploración bajo demanda y habilite la exploración dinámica.

Planificación de exploración

En IBM QRadar Vulnerability Manager, puede planificar las fechas y horas de exploración de 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 utilizando ventanas operativas para configurar las horas de exploración permitidas.

Elija una de las siguientes opciones de planificación:

- Manual
- Ejecutar una vez
- Diariamente
- Semanalmente
- Mensualmente
- Avanzada

  Utilice expresiones cron para crear planificaciones, por ejemplo, de lunes a viernes a las 9:00 AM o a las 3:30 AM el primer viernes de cada mes. Las expresiones cron ofrecen la posibilidad de crear planificaciones de exploración irregulares. Planifique un máximo de una exploración por día.

Tenga en cuenta el impacto de los cambios generados por el horario de verano en las planificaciones de exploración **Ejecutar una vez**, **Diariamente**, **Semanalmente** y **Mensualmente**. Por ejemplo el 27 de marzo de 2016, los relojes del Reino Unido se adelantan 1 hora a la 1:00 AM, por lo que las exploraciones configuradas para ejecutarse entre la 1:00 AM y la 1:59 AM del 27 de marzo de 2016 se ejecutarán entre las 2:00 AM y las 2:59 AM.

Las planificaciones de exploración de tipo **Avanzada** configuradas para ejecutarse entre la 1:00 AM y la 1:59 AM del 27 de marzo de 2016 se omiten y no se ejecutan. Todas las exploraciones posteriores se ejecutan a la hora prevista.

Tareas relacionadas

Configurar un intervalo de exploración permitida

Revisar las exploraciones planificadas en formato de calendario

Explorar dominios mensualmente

En IBM 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. 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 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

Revisar las exploraciones planificadas en formato de calendario

En IBM 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. 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. Haga una doble pulsación sobre una exploración planificada para editar el perfil de exploración.

Destinos y exclusiones de la exploración de red

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

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

Planificar exploraciones de activos nuevos no explorados

Explorar dominios mensualmente

Excluir activos en todas las exploraciones

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

Puede configurar los protocolos de puertos del perfil de exploración utilizando las opciones de exploración de TCP y UDP.

Configure los protocolos de exploración y los puertos que desee explorar en la pestaña **Exploración de puertos** de una ventana de configuración de política de exploración nueva o existente.

Nota: También puede configurar la exploración de puertos desde la pestaña **Cómo explorar** de la ventana **Configuración de perfil de exploración**, pero esta opción sólo está habilitada para la retrocompatibilidad. No utilice la pestaña **Cómo explorar** para configurar nuevas exploraciones de puertos.

Explorar un rango de puertos completo

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

Acerca de esta tarea

Cree una política de exploración para especificar los puertos que desee explorar, y luego añada esta política de exploración a un perfil de exploración que utilizará para ejecutar la exploración.

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** para crear una nueva política de exploración o **Editar** para editar una política existente.
4. Pulse la pestaña **Valores**.
   a) Escriba un nombre y una descripción para la política de exploración.
   b) Seleccione el tipo de exploración.
5. Pulse la pestaña **Exploración de puertos**.
6. En el campo **Protocolo**, seleccione un protocolo. Los valores predeterminados son **TCP y UDP**.

   Nota: Las exploraciones de puertos UDP son mucho más lentas que las exploraciones de puertos TCP debido al funcionamiento de UDP. Una exploración de puertos UDP puede tardar hasta 24 horas en explorar todos los puertos (1-65535) de un activo.
7. 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).
8. 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.

9. Opcional: Configure más opciones en otras pestañas si desea utilizar la política de exploración para realizar más tareas.
10. Pulse **Guardar**.
11. En la página **Perfiles de exploración**, cree un perfil de exploración.
    a) Añada la política de exploración que ha guardado.
    b) Configure los parámetros restantes para el perfil de exploración y guárdelo.
    c) En la página **Perfiles de exploración**, seleccione el perfil de exploración nuevo y, a continuación, pulse **Ejecutar** en la barra de herramientas para ejecutar la exploración.

    Para obtener más información sobre cómo crear un perfil de exploración, consulte "Crear un perfil de exploración" en la página 39.

    Nota: También puede configurar la exploración de puertos desde la pestaña **Cómo explorar** de la ventana **Configuración de perfil de exploración**, pero esta opción sólo está habilitada para la retrocompatibilidad. No utilice la pestaña **Cómo explorar** para configurar nuevas exploraciones de puertos.

Explorar activos con puertos abiertos

En IBM 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 41.

Configurar un intervalo de exploración permitida

En IBM 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. Elija una planificación de intervalo operativo en la lista **Planificación**.
6. Seleccione los días en que se puede realizar la exploración.
7. Seleccione su zona horaria.
8. Si ha seleccionado **Semanal** en la lista **Planificación**, marque los recuadros de selección de los días de la semana deseados en el área **Semanal**.
9. Si ha seleccionado **Mensualmente** en la lista **Planificación**, seleccione un día en la lista **Día del mes**.
10. 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 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 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 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 8.
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

Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager

Detalles de perfil de exploración

Tareas relacionadas

Creación de un perfil de exploración bajo demanda

Para desencadenar una exploración en respuesta a un suceso de reglas personalizadas, configure un perfil de exploración bajo demanda y habilite la exploración dinámica.

Asociar exploraciones de vulnerabilidades a rangos de CIDR

En IBM 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 8.

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

Tareas relacionadas

Creación de un perfil de exploración bajo demanda

Para desencadenar una exploración en respuesta a un suceso de reglas personalizadas, configure un perfil de exploración bajo demanda y habilite la exploración dinámica.

Explorar rangos de CIDR con exploradores de vulnerabilidades diferentes

En IBM 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 8.

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. 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**.

Tareas relacionadas

Creación de un perfil de exploración bajo demanda

Para desencadenar una exploración en respuesta a un suceso de reglas personalizadas, configure un perfil de exploración bajo demanda y habilite la exploración dinámica.

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

Configuración de una política de exploración
En IBM QRadar Vulnerability Manager,puede configurar una política de exploración para ajustarse a los requisitos específicos de sus exploraciones de vulnerabilidad. Puede copiar y renombrar una política de exploración preconfigurada o puede añadir una política de exploración nueva. No puede editar una política de exploración preconfigurada.

Actualizaciones automáticas de política de exploración para vulnerabilidades críticas

Como parte de las actualizaciones automáticas diarias de IBM 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 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**.

Configuración de una política de exploración

En IBM QRadar Vulnerability Manager,puede configurar una política de exploración para ajustarse a los requisitos específicos de sus exploraciones de vulnerabilidad. Puede copiar y renombrar una política de exploración preconfigurada o puede añadir una política de exploración nueva. No puede editar una política de exploración preconfigurada.

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, debe configurar como mínimo los campos obligatorios de la ventana **Política de exploración nueva** que son **Nombre** y **Descripción**.
5. En la lista **Tipo de exploración** seleccione el tipo de exploración.
6. Para gestionar y optimizar el proceso de descubrimiento de activos, pulse la pestaña **Descubrimiento de activos**.
7. Para gestionar los puertos y protocolos que se utilizan para una exploración, pulse la pestaña **Exploración de puertos**.
8. Para incluir vulnerabilidades específicas en la política de exploración de parches, pulse la pestaña **Vulnerabilidades**.

   Nota: La pestaña **Vulnerabilidades** solo está disponible cuando selecciona una exploración de parches.
9. Para incluir o excluir grupos de herramientas de la política de exploración, pulse la pestaña **Grupos de herramientas**.

   Nota: La pestaña **Grupos de herramientas** sólo está disponible cuando se selecciona una política de exploración completa plus o de exploración completa de cero credenciales.
10. Para incluir o excluir herramientas de una política de exploración, pulse la pestaña **Herramientas**.

    Nota: La pestaña **Herramientas** sólo está disponible cuando se selecciona una política de exploración completa plus o de exploración completa de cero credenciales.

    Importante: Si no modifica las herramientas o grupos de herramientas y selecciona la opción **Completa**, todas las herramientas y grupos de herramientas que están asociados a una exploración completa se incluyen en la política de exploración.
11. Pulse **Guardar**.

Capítulo 6. Gestión de falsos positivos

Normalmente, en la exploración de vulnerabilidades los falsos positivos se producen cuando el explorador sólo puede acceder a un subconjunto de la información necesaria, lo cual le impide determinar con precisión si existe una vulnerabilidad.

Para ayudar a reducir el número de falsos positivos, debe configurar los exploradores con las credenciales adecuadas. Las exploraciones necesitan acceso a toda la información de activos necesaria para que el usuario pueda determinar con exactitud si existe una vulnerabilidad.

¿Por qué se producen falsos positivos?

Un falso positivo puede producirse cuando el explorador sólo puede leer la información de configuración de banners de servicio. Por ejemplo, un explorador que lee un banner de Apache puede detectar que sólo está instalada la versión 2.2.15 a partir de la cabecera HTTP, aunque también esté instalada la versión 2.2.15-39 y que la versión contenga un arreglo de software que se ha actualizado.

Otro ejemplo es cuando el explorador lee el banner y detecta la versión de SSH instalada, pero no puede detectar el nivel de parche o el sistema operativo. Si el explorador detecta que está instalado SSH-2, pero no puede determinar el sistema operativo, no puede determinar con precisión si existe una vulnerabilidad en algunos casos. La vulnerabilidad podría identificarse correctamente en un activo, pero ser un falso positivo en el otro activo porque las vulnerabilidades de SSH en Red Hat SSH podrían no ser las mismas para otros sistemas operativos Linux.

Por qué los exploradores no recuperan toda la información necesaria

Los exploradores de vulnerabilidades no siempre pueden acceder a la información que necesitan para determinar con precisión si existe una vulnerabilidad. Esta limitación genera habitualmente falsos positivos.

El explorador no puede autenticarse

Si el explorador no puede autenticarse en el punto final, debe basarse en la información limitada procedente del sondeo de servicios de red anónimos, como por ejemplo la información recuperada de la lectura de banners.

Los banners podrían contener versiones incorrectas e información de nivel de parche obsoleta, lo cual genera falsos positivos. Sin embargo, si el explorador puede autenticarse, puede determinar la versión completa del sistema operativo y la información de nivel de parches, y luego suprimir las vulnerabilidades de falsos positivos.

Procedimientos recomendados con respecto a los banners

Utilice estos procedimientos recomendados sobre los banners cuando configure la exploración de vulnerabilidades en la red:

- No incluya información detallada o confidencial en un banner, ya que un pirata informático puede obtener información crucial sobre las aplicaciones y servicios que se están ejecutando en un activo y luego utilizar vulnerabilidades conocidas para explotarlas.
- Conozca el tipo de información que está disponible de forma anónima en los banners. Evalúe los vectores de intentos de ataque más probables. Esta información es de utilidad para evaluar la seguridad de red y para recopilar información de red.
- Marque la información de vulnerabilidad que se lee en los banners como falsos positivos etiquetando la vulnerabilidad como una excepción desde pestañas como el panel **Instancias de vulnerabilidad** de la ventana **Detalles de activo** o la ventana **Historial de vulnerabilidades**.
- Ajuste las exploraciones habilitando o inhabilitando herramientas de las políticas de exploración que puedan evitar el inicio de estas exploraciones.

Técnicas de exploración basada en Windows autenticada

La exploración basada en Windows autenticada utiliza las dos técnicas siguientes para detectar vulnerabilidades:

- Exploración de registro, donde el explorador necesita acceso al registro.
- Exploración OVAL, donde WMI (Windows Management Instrumentation) debe configurarse correctamente.

Si una de estas dos técnicas falla, el resultado de la exploración es propenso a generar falsos positivos.

Debe habilitar el servicio de registro remoto para que el explorador acceda al registro.

La configuración errónea de WMI (Windows Management Instrumentation) puede generar falsos positivos.

Identificar anomalías de autenticación

Si una exploración no se autentica correctamente, pase el curso por encima del símbolo de aviso para ver por qué la exploración ha encontrado problemas. Por ejemplo,

```
La última exploración de este activo ha fallado
STATUS_LOGON_FAILURE
Por tanto, la vulnerabilidad puede no ser exacta
```

Otros ejemplos de mensajes de aviso son `Anomalía de inicio de sesión de SSH`, `servicio de registro remoto no iniciado` y `sin acceso WMI`.

Conceptos relacionados

Exploración de activos basados en Windows

QRadar Vulnerability Manager utiliza la exploración de registro y la exploración OVAL (Open Vulnerability Assessment Language) para detectar vulnerabilidades en activos basados en Windows. Utilice exploraciones autenticadas para detectar todas las vulnerabilidades en Windows. Es posible que las exploraciones no autenticadas no detecten todas las vulnerabilidades en Windows.

Tareas relacionadas

Configurar una exploración autenticada del sistema operativo Windows

Habilitación de permisos para exploración de parches de Linux o UNIX

Aplicar una regla de excepción de vulnerabilidad

¿Cómo se detecta el resultado de la exploración de vulnerabilidades?

Determine si el resultado de la exploración de vulnerabilidades se genera a partir de una exploración autenticada o desde una lectura anónima de un banner. Los resultados de exploración generados desde una lectura anónima de un banner es más probable que sean falsos positivos.

Pase el cursor por encima de la columna **Detalles** del resultado de la exploración de vulnerabilidades del activo para ver cómo se detecta la vulnerabilidad.

1. Pulse la pestaña **Vulnerabilidades**.
2. En el menú de navegación, pulse **Resultados de exploración**.
3. Efectúe una doble pulsación en un perfil de exploración en la columna **Nombre**.
4. Pulse cualquier fila de la columna **Instancias de vulnerabilidad**.
5. Pase el cursor por encima de un resultado en la columna **Detalles** para ver más detalles.

   Por ejemplo, puede que se generan los siguientes detalles cuando el explorador lee un banner:

   ```
   SERVER: Apache/2.2.15(Red Hat)
   ```

Exploraciones de parches y falsos positivos

Las vulnerabilidades detectadas por exploraciones de parches no es probable que sean falsos positivos, excepto las actualizaciones de KB de Windows. Las actualizaciones de Windows, que tienen como prefijo

un número de base de conocimiento (KB), pueden ser falsos positivos cuando la fase WMI (Windows Management Instrumentation) de la exploración autenticada de Windows falla.

Las actualizaciones de Windows se reemplazan a lo largo del tiempo. Por ejemplo, un KB de Windows actual reemplaza al KB inicial que solucionaba un arreglo de vulnerabilidad original. La sustitución no es un problema para las actualizaciones de Windows recientes o cuando la exploración de WMI u OVAL es satisfactoria, ya que la exploración tiene en cuenta las actualizaciones más recientes.

Investigar un falso positivo potencial de una exploración autenticada

A veces, una exploración autenticada genera un falso positivo porque la exploración falla.

Acerca de esta tarea

Investigue la vulnerabilidad.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el menú de navegación, pulse **Resultados de exploración**.
3. En la ventana **Resultados de exploración**, pulse una fila de la columna Vulnerabilidades.
4. Pulse la vulnerabilidad que desee investigar.
5. Pulse el enlace **Detalles de plugin** para abrir la ventana de parches para la vulnerabilidad.
6. Utilice las pestañas para descubrir información preventiva de Oval Definition, Windows Knowledge Base o UNIX sobre la vulnerabilidad.
   - Para las vulnerabilidades creadas desde una prueba OVAL (Open Vulnerability and Assessment Language), pulse la pestaña **OVAL** adecuada para ver los criterios que QRadar Vulnerability Manager utiliza en la prueba.
   - Para las vulnerabilidades que se crean desde una exploración de registro de KB de Windows, pulse la pestaña **KB de Windows** para ver las actualizaciones (KB) que QRadar Vulnerability Manager asocia con la vulnerabilidad.
   - Para las vulnerabilidades que se crean debido a que falta un RPM Package Manager (RPM), pulse la pestaña **Unix**. Los paquetes y revisiones visualizados se comparan con los releases de los sistemas operativos adecuados.

Capítulo 7. Exploraciones de parches autenticadas

En IBM 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. Esta función se aplica a SNMP V1 y V2c.

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 los sistemas operativos Windows en busca de los parches que faltan, se deben habilitar el acceso de registro remoto y Windows Management Instrumentation (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`.

Habilitar algunas restricciones para los clientes RPC autenticados en su Política de grupo de Windows impide que QRadar Vulnerability Manager ejecute consultas WMI cuando explore un servidor de Windows. Cuando se produzca este error de autenticación, se mostrará un triángulo de color amarillo junto al activo en los resultados de la exploración. Por ejemplo, si habilita **Restringir cliente RPC sin autenticar** en Windows 2012, podrá seleccionar **Ninguno**, **Autenticado** o **Autenticado sin excepciones** en el menú. Si selecciona **Autenticado sin excepciones**, QRadar Vulnerability Manager no podrá ejecutar consultas WMI y no podrá finalizar la exploración.

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 claves públicas en cada sistema operativo Linux que explore.

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

Configurar una exploración autenticada de los sistemas operativos Linux o UNIX

Configurar una exploración autenticada del sistema operativo Windows

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

Configurar una exploración autenticada del sistema operativo Windows

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.

Configurar un conjunto de credenciales

En IBM 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. En el menú de navegación (☰), pulse **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. 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 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 instalar una clave pública y privada en un explorador de QVM e instalar la clave pública en el destino de exploración.

Un escáner de QVM se instala automáticamente en un host de procesador de QVM y también se puede instalar en otros hosts gestionados.

La cuenta de usuario en el destino de exploración debe tener un shell de inicio de sesión y debe ser capaz de ejecutar los mandatos que son necesarios para una exploración de parches en el destino. Para obtener más información, consulte "Habilitación de permisos para exploración de parches de Linux o UNIX" en la página 65.

Este procedimiento describe cómo configurar un único par de claves pública/privada y transferirlas a un explorador de QVM y destino de exploración.

Procedimiento

1. Utilizando SSH, inicie la sesión en la consola de QVM como usuario root.
2. Genere un par de clave pública escribiendo el mandato siguiente:

   ```
   su -m -c 'ssh-keygen -t <tipo_clave>' qvmuser
   ```

   Nota: *<tipo_clave>* es dsa o rsa.
3. Acepte el archivo predeterminado pulsando **Intro**.
4. Acepte la contraseña predeterminada para la clave pública pulsando **Intro**.
5. Pulse **Intro** de nuevo para confirmar.
6. Copie las claves pública y privada en todos los hosts gestionados en los que se instala un escáner de QVM.

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   rsync -ogp id_<tipo_clave> id_<tipo_clave>.pub <dirección IP>:/home/
   qvmuser/.ssh
   ```

   - Sustituya *<tipo_clave>* con dsa o rsa.
   - Sustituya *<dirección IP>* por la dirección IP del escáner y escriba la contraseña de root cuando se le solicite.

   Nota: El procesador de QVM incluye un escáner. Si el procesador no se ejecuta en la consola de QRadar, también debe transferir las claves al procesador de QVM.
7. Copie la clave pública en el destino de exploración escribiendo el mandato siguiente:

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   ssh-copy-id -i id_<tipo_clave>.pub <usuario>@<dirección IP>
   ```

   - *<tipo_clave>*: dsa o rsa.
   - *<dirección IP>*: la dirección IP del destino de exploración.
   - *<usuario>*: el usuario en el destino de exploración.
8. Escriba la contraseña de usuario para el destino de exploración.
9. Compruebe que la cuenta *qvmuser* en el escáner QVM puede utilizar SSH en el destino de exploración sin una contraseña, escribiendo el mandato siguiente:

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no <usuario>@<dirección IP> ls'
   qvmuser
   ```

   - *<dirección IP>*: la dirección IP del destino de exploración.
   - *<usuario>*: el usuario en el destino de exploración.

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

Qué hacer a continuación

Cree un perfil de exploración en QRadar Vulnerability Manager con el nombre del usuario en el destino de exploración sin especificar una contraseña y ejecute una exploración de parches.

Tareas relacionadas

Configurar una exploración autenticada de los sistemas operativos Linux o UNIX

Configurar una exploración autenticada de los sistemas operativos Linux o UNIX

En IBM 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 62.

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. 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 QVM no puede encontrar un conjunto de credenciales centralizado para los hosts que está explorando, utiliza las credenciales existentes que se especifican manualmente en la pestaña **Credenciales adicionales**.
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

Tareas relacionadas

Configurar un conjunto de credenciales

En IBM 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

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

Realice las siguientes tareas para comprobar que la cuenta de usuario que utilice con la exploración tenga los permisos necesarios para la exploración de parches de Linux o UNIX.

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:

Tabla 9. Mandatos para ejecutarse en el sistema operativo

Sistema operativo	Mandatos

Linux	Los archivos siguientes contienen el contenido relevante para su distribución:
	/etc/redhat-release
	/etc/SuSE-release
	/etc/debian-version
	/etc/slackware-version
	/etc/mandrake-version
	/etc/gentoo-version
	Por ejemplo, en Red Hat Enterprise Linux, utilice los mandatos:
	`ls /etc/redhat-release`
	`cat/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Tabla 9. Mandatos para ejecutarse en el sistema operativo (continuación)

Sistema operativo	Mandatos

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`

Consejo:

Como práctica recomendada, desactive las notificaciones por correo electrónico para la cuenta de usuario de exploración porque la notificación por correo electrónico puede interferir con el proceso de los resultados de exploración. Vea la documentación del sistema operativo para obtener detalles sobre cómo desactivar las notificaciones por correo electrónico para cuentas de usuario.

Capítulo 8. Exploración de activos basados en Windows

QRadar Vulnerability Manager utiliza la exploración de registro y la exploración OVAL (Open Vulnerability Assessment Language) para detectar vulnerabilidades en activos basados en Windows. Utilice exploraciones autenticadas para detectar todas las vulnerabilidades en Windows. Es posible que las exploraciones no autenticadas no detecten todas las vulnerabilidades en Windows.

¿Cuándo son visibles las actualizaciones de datos de vulnerabilidad en QRadar?

Las vulnerabilidades recién publicadas son visibles en el panel de control de QRadar Vulnerability Manager y en la sección de investigación de la pestaña **Vulnerabilidad** de QRadar.

QRadar Vulnerability Manager obtiene actualizaciones de vulnerabilidad diarias, que incluyen noticias, avisos, vulnerabilidades recién publicadas y sus metadatos asociados, datos de prueba y cualquier nueva detección.

Los sistemas de QRadar Vulnerability Manager se actualizan normalmente con las vulnerabilidades más recientes 2-3 días después de anunciarlas.

¿Qué tipos de métodos de exploración están disponibles?

La lista siguiente describe los puntos importantes sobre los métodos de exploración que están disponibles para detectar vulnerabilidades en activos basados en Windows:

Exploraciones autenticadas o no autenticadas
Debe utilizar exploraciones autenticadas para detectar todas las vulnerabilidades basadas en Windows. Si utiliza una exploración no autenticada para detectar vulnerabilidades basadas en Windows, los resultados pueden no ser completos y ser propensos a proporcionar falsos positivos.

Exploraciones de registro
La exploración de registro se utiliza para detectar vulnerabilidades en el sistema operativo Windows.

- QRadar Vulnerability Manager utiliza el servicio de registro remoto y Windows Management Instrumentation (WMI) para recuperar información sobre los paquetes de servicio KB instalados, el software instalado y los servicios habilitados desde los puntos finales explorados, y esta información se correlaciona con definiciones de vulnerabilidad.
- Cada definición de vulnerabilidad de Windows incluye el boletín, KB, producto, sistema operativo, paquete de servicio y el servicio de Windows necesario.

Exploraciones OVAL (Open Vulnerability Assessment Language)
La exploración OVAL (Open Vulnerability Assessment Language) se utiliza para detectar vulnerabilidades en el sistema operativo Windows.

OVAL (Open Vulnerability Assessment Language) es un estándar al que se hace referencia al realizar pruebas OVAL para vulnerabilidades y pruebas de configuración en activos. La lista siguiente describe información sobre vulnerabilidades y pruebas OVAL.

- Las pruebas pueden incluir cualquier combinación de claves de registro, valores de clave de registro, versiones de `.dll` y `.exe`, servicios en ejecución, presencia de archivos.
- Cada definición de vulnerabilidad es una expresión lógica XML que determina si el sistema es vulnerable.
- Se prueban todas las versiones de `.exe` y `.dll`.
- Puede pulsar el enlace de CVE correspondiente a una vulnerabilidad para ver si tiene una prueba OVAL, por ejemplo, CVE-2013-3910 (https: //web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3910)

- Las definiciones de pruebas de OVAL están disponibles en línea en el sitio web de Oval, (https://oval.cisecurity.org/)
- La prueba de OVAL puede alterar temporalmente una vulnerabilidad generada.

Exploraciones de parches del SO Windows

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

Las exploraciones de parches realizan una exploración limitada de los puertos Nmap 22, 139, y 445, para determinar si el activo es un activo de Windows o UNIX. Si la exploración de puertos descubre los puertos NetBIOS 139 o 445, sabe que estos puertos corresponden a un activo basado en Windows. La herramienta de vulnerabilidad de enumeración se utiliza para explorar un activo de Windows.

Las exploraciones de parches no son invasivas y no realizan pruebas de vulnerabilidad activa.

Las exploraciones de parches se factorizan en parches reemplazados automáticamente.

Es posible explorar sistemas en busca de parches del SO Windows sin configurar WMI (Windows Management Instrumentation) y Recursos compartidos administrativos, pero los resultados no son completos y son propensos a proporcionar positivos falsos.

Requisitos de configuración para la exploración de activos basados en Windows

La lista siguiente describe los requisitos que debe configurar para la exploración de activos basados en Windows:

- Configurar el acceso a registro remoto en los activos.
- Configurar Windows management instrumentation (WMI) en los activos.
- Para leer datos de WMI en un servidor remoto a través de un cortafuegos, debe permitir solicitudes WMI a través de un cortafuegos de Windows.
- Si utiliza una cuenta no administrativa para supervisar el servidor Windows, debe establecer permisos de DCOM mínimos y otorgar permisos de acceso remoto a DCOM para esa cuenta no administrativa.
- Configurar unidades compartidas administrativas en los activos.

Configurar una exploración autenticada del sistema operativo Windows

En IBM 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.

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. 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 QVM no puede encontrar un conjunto de credenciales centralizado para los hosts que está explorando, utiliza las credenciales existentes que se especifican manualmente en la pestaña **Credenciales adicionales**.
5. Pulse el panel **Cuándo explorar**.
6. En la lista **Ejecutar planificación**, seleccione **Manual**.

   Si desea que la exploración se ejecute en un momento posterior, elija una de las opciones de **Planificación de ejecución** disponibles.
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 (**>**).

   El nombre de dominio que teclea es el dominio de Windows, no un dominio interno.
9. Pulse **Guardar**.
10. En la página **Perfiles de exploración**, pulse **Ejecutar**.

Conceptos relacionados

Conjuntos de credenciales centralizadas

Exploraciones de parches autenticadas

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 WMI

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 Windows Management Instrumentation (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.

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 shell y especifique el mandato siguiente:

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

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. 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.

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 configurar 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 los permisos de acceso remoto en el sistema B para permitir a un grupo que no sea miembro del grupo de administradores del sistema B se conecte remotamente 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 la sección **Permisos de acceso**, pulse **Editar límites**.
5. Configure uno de los usuarios o grupos siguientes para que tengan derechos de acceso remoto.
   - En el cuadro de diálogo **Permiso de acceso**, seleccione el nombre **ANONYMOUS LOGON** en el cuadro **Nombres de grupo o usuario**. En el área **Permisos para ANONYMOUS LOGON** marque el recuadro de selección **Permitir** para **Acceso remoto** y a continuación pulse **Aceptar**.
   - En el cuadro de diálogo **Permiso de acceso**, seleccione el nombre **Todos** en el cuadro **Nombres de grupo o usuario**. En el área **Permisos para todos** marque el recuadro de selección **Permitir** para **Acceso remoto** y a continuación pulse **Aceptar**.
   - En el cuadro de diálogo **Permiso de acceso**, seleccione el nombre **<usuario de exploración de QVM>** en el cuadro **Nombres de grupo o usuario**. En el área **Permisos para <usuario de exploración de QVM>** marque el recuadro de selección **Permitir** para **Acceso remoto** y a continuación pulse **Aceptar**.

   Nota: Si desea utilizar la cuenta de usuario **<usuario de exploración de QVM>**, debe crear la cuenta de usuario antes de otorgar derechos de acceso remoto de DCOM. También debe configurar acceso WMI (paso 6) para este usuario.

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$.

Configuración manual de la autenticación NTLMv2 para evitar anomalías de exploración

Debe configurar manualmente las exploraciones con credenciales que puede ejecutar contra activos que utilizan Microsoft New Technology LAN Manager versión 2 (NTLMv2) para poder evitar que las exploraciones fallen.

Acerca de esta tarea

Cuando ejecuta una exploración con credenciales contra un activo de Windows que utiliza el nivel de autenticación de LAN Manager `"Send NTLMv2 response only. Refuse LM and NTLM"`, es posible que algunas de las herramientas de exploración no puedan autenticarse. Se visualiza un triángulo de aviso amarillo para el activo y surge una vulnerabilidad de error de comprobaciones locales. Si la exploración se ejecuta varias veces, la cuenta del usuario puede quedar bloqueada en el activo.

Para evitar que las exploraciones que se ejecutan contra activos que utilizan NTMLv2 fallen, habilite manualmente la autenticación NTMLv2 en los archivos siguientes del Explorador de QVM:

- `/opt/qvm/etc/smb.conf`
- `/opt/qvm/etc/smb.conf.smbv1`
- `/opt/qvm/etc/smb.conf.smbv2`

Procedimiento

Abra cada uno de estos archivos y añada la línea siguiente: `client ntlmv2 auth = yes`

Capítulo 9. Reglas de excepción de vulnerabilidad

En IBM 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.

Consejo: La tabla **Reglas de excepción** muestra solamente el comentario más reciente que se ha entrado. Para ver los otros comentarios, pase el cursor por encima de la columna **Comentario** de la regla.

Tareas relacionadas

Reducir el número de vulnerabilidades de falso positivo

Aplicar una regla de excepción de vulnerabilidad

En IBM 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. 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**.
7. En el campo **Regla de excepción**, seleccione una opción de caducidad.
8. Para proporcionar una razón para la excepción, seleccione una razón de la lista **Razón**.
9. En el campo **Activos**, seleccione los activos de destino para la regla de excepción eligiendo una de las opciones siguientes:
   - Para aplicar la excepción a todos los activos, seleccione **Vulnerabilidad de excepción para todos los activos**.
   - Para aplicar la excepción a un activo específico, seleccione **Excepción para activo específico con IP actual**.

     De forma predeterminada, se selecciona el activo que está asociado con la vulnerabilidad que ha seleccionado en el paso 5.
   - Para aplicar la excepción a una dirección IP específica, CIDR, o red, especifique los detalles, seleccione el dominio y pulse **Añadir**.

Si selecciona una red específica de la jerarquía de red, la excepción sólo se aplica a las direcciones IP en esa red. Por ejemplo, si una dirección IP está asignada a dos redes de la jerarquía de red, la excepción no se aplica a esa misma dirección IP en segunda red, a menos que se especifique como una excepción.

10. En el campo **Notas**, especifique los comentarios en el recuadro de texto **Comentarios**.
11. Pulse **Guardar** o **Cancelar**.

Conceptos relacionados

Gestión de falsos positivos

Normalmente, en la exploración de vulnerabilidades los falsos positivos se producen cuando el explorador sólo puede acceder a un subconjunto de la información necesaria, lo cual le impide determinar con precisión si existe una vulnerabilidad.

Tareas relacionadas

Buscar 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 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 10. Investigaciones de exploración

En IBM 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. La columna **Puntuación** muestra la puntuación CVSS (Common Vulnerability Scoring System) para el perfil de exploración completado. Se incluye la puntuación base y temporal CVSS en el cálculo de esta puntuación, pero la puntuación ambiental CVSS no se incluye en este cálculo. La puntuación ambiental CVSS se incorpora en la columna **Puntuación de riesgo** que puede ver en la ventana **Gestionar vulnerabilidades**.
- 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.

Nota: El progreso de la exploración puede indicar que la exploración se ha completado al 100% mientras se siguen procesando los resultados. Para ver si ha finalizado el proceso, pase el cursor por encima de la barra de progreso.

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 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 IBM QRadar Vulnerability Manager, puede planificar las fechas y horas de exploración de 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 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. 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. 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. 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**.

Volver a publicar resultados de exploración

Si el modelo de activo no se actualiza automáticamente con resultados de una exploración completada, puede volver a publicarlos manualmente desde la página **Resultados de la exploración**.

Acerca de esta tarea

Si no ha marcado el recuadro de selección **Update Asset Model** al configurar un perfil de exploración, los resultados de exploración no se publican automáticamente en el modelo de activo. Puede actualizar manualmente el modelo de activo con resultados de de exploración para ese perfil.

Procedimiento

1. Vaya a **Vulnerabilidades** > **Resultados de exploración**
2. Pulse el recuadro de selección en la fila asignada a los resultados de exploración que desea volver a publicar.
3. Pulse **Republish** en la barra de herramientas de la página **Resultados de exploración** y a continuación pulse **Aceptar**.

   Una columna **Tipo** indica que el modelo de activo no se actualiza con los resultados de la exploración seleccionados. El icono de aviso rojo desaparece una vez completado el proceso de publicación.
4. Mueva el puntero del ratón sobre la columna **Tipo** para ver la confirmación en la ayuda contextual de que el modelo de activo se ha actualizado para los resultados de exploración seleccionados.

   Nota: Puede volver a publicar varios resultados de exploración al mismo tiempo. Sin embagor, si ha vuelto a publicar dos conjuntos de resultados de exploración del mismo perfil, el modelo de activo se actualiza solo con el último conjunto de resultados de exploración.

   Si ha configurado la generación automática de informes en la pestaña **Email** de la página **Scan Profile Configuration**, los informes se generan y se envían a las direcciones de correo electrónico configuradas al volver a publicar resultados de exploración.

Niveles de riesgo de activos y categorías de vulnerabilidades

En IBM 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 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

Reglas de excepción de vulnerabilidad

En IBM 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 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**.

Resolución de problemas de exploración

Resolución de problemas de exploración en la red mediante investigación de registros, y mensajes de error y aviso.

Tiempo de respuesta lento de host explorado
Despliegue el dispositivo de exploración de QRadar Vulnerability Manager relativamente cerca de los activos que está explorando. Utilice mandatos como traceroute para asegurarse de que los paquetes alcanzan el activo en menos de 50 ms; de lo contrario, las exploraciones pueden tardar mucho tiempo.

Comprobar el estado de las herramientas de exploración

Si las exploraciones se ejecutan durante mucho tiempo y desea saber qué herramientas se están ejecutando, pase el cursor por encima del porcentaje de progreso de exploración en la página de resultados de exploración para visualizar una ventana emergente, que le muestra la herramienta activa.

La exploración de parches no se conecta a un activo de Linux
Si la herramienta de exploración de parches no se conecta a un activo de Linux, aparece un icono de aviso triangular amarillo junto al activo en los resultados de exploración.

Es posible que vea el mensaje de error SSH `Patch Scanning-Failed Logon`.

Valide el nombre de usuario y la contraseña. Si está utilizando el cifrado de clave pública, compruebe la clave pública.

Para explorar sistemas operativos Linux utilizando la autenticación segura, configure el cifrado de clave pública entre la consola o el host gestionado y los destinos de exploración. 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. Para obtener más información, consulte Capítulo 7, “Exploraciones de parches autenticadas”, en la página 61.

Error de comprobaciones locales

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.

Es posible que vea el mensaje de error `Local Checks Error`, que significa que la exploración autenticada ha fallado.

Puede configurar credenciales en el perfil de exploración o en credenciales centralizadas. Si el explorador está explorando hosts basados en Windows, los tres servicios siguientes de Windows deben estar configurados correctamente:

- Registro remoto
- Windows Management Instrumentation (WMI)
- Comparticiones de admin

Para obtener más información, consulte Capítulo 8, “Exploración de activos basados en Windows”, en la página 67.

Mismos títulos de vulnerabilidad para diferentes KB

Si el KB para un boletín es reemplazado por un KB en un boletín futuro, el título de vulnerabilidad no cambia.

Exploración encallada

Si la exploración se detiene o es intermitente, un usuario autorizado puede iniciar sesión en el explorador y verificar la conectividad con el procesador de exploración. Consulte en los registros de errores de QRadar Vulnerability Manager si hay errores de conexión.

La exploración de puertos UDP tarda mucho tiempo

Si una política de exploración está configurada para explorar todos los puertos UDP, la exploración puede tardar mucho tiempo en completarse, especialmente si el host de destino tiene varios puertos UDP cerrados. Para exploraciones de conformidad PCI, no es necesario explorar todos los puertos UDP. Para obtener más información, consulte “Duración de la exploración y exploración de puertos” en la página 30.

Advertencia de número de activos explorados

Si ve el siguiente mensaje de advertencia en la pantalla **Resultados de exploración**, el rendimiento y los resultados de la exploración no se ven afectados:

AVISO: Ha explorado *<número>* activos pero sólo tiene licencia para explorar *<número>* activos. Es necesaria la actualización de licencia.

Nota: Es posible que necesite comprobar la licencia de QRadar Vulnerability Manager para verificar cuántos activos le permite explorar su licencia.

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 *Guía de administración de IBM QRadar*.

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 11. Gestión de vulnerabilidades

En IBM 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.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) se utiliza para valorar la gravedad y el riesgo de seguridad del sistema.

CVSS es un entorno abierto que consta de los siguientes grupos de métricas:

- Base
- Temporal
- Del entorno

Base
El rango de gravedad de puntuación base es de 0 a 10 y representa las características inherentes de la vulnerabilidad. La puntuación base tiene la mayor relevancia en la puntuación CVSS final y puede dividirse adicionalmente en las siguientes subpuntuaciones:

- Efecto

  La subpuntuación de impacto representa medidas de impacto de confidencialidad, impacto de integridad e impacto de disponibilidad de una vulnerabilidad explotada satisfactoriamente.
- Explotabilidad

  La subpuntuación de explotabilidad representa métricas para vector de acceso, complejidad de acceso y autenticación, y mide cómo se accede a la vulnerabilidad, la complejidad del ataque, y el número de veces que un atacante se debe autenticar para explotar con éxito una vulnerabilidad.

Temporal

La puntuación temporal representa las características de una amenaza de vulnerabilidad que cambian con el tiempo, y consta de las siguientes medidas:

- Explotabilidad

  La disponibilidad de técnicas o código que se puede utilizar para explotar la vulnerabilidad, que cambia con el tiempo.

- Nivel de remediación

  El nivel de remediación disponible para una vulnerabilidad.
- Confianza en el informe

  El nivel de confianza en la existencia de la vulnerabilidad y la credibilidad de sus detalles técnicos.

Del entorno

La puntuación del entorno representa características de la vulnerabilidad afectadas por el entorno del usuario. Configure las siguientes medidas del entorno para resaltar las vulnerabilidades de activos importantes o críticos aplicando medidas del entorno más elevadas. Aplique las puntuaciones más altas para los activos más importantes porque las pérdidas que están asociadas a estos activos tienen mayores consecuencias para la organización.

- Potencial de daños colaterales (CDP)

  El potencial de pérdida de vidas humanas o activos físicos a través de daños o el robo de este activo, o la pérdida económica de productividad o ingresos.
- Distribución de destino (TD)

  La proporción de sistemas vulnerables en el entorno del usuario.
- Requisito de confidencialidad (CR)

  El nivel de impacto en la pérdida de confidencialidad cuando se explota una vulnerabilidad en este activo.
- Requisito de integridad (IR)

  Esta métrica indica el nivel de impacto en la pérdida de integridad cuando se explota una vulnerabilidad con éxito en este activo.
- Requisito de disponibilidad (AR)

  El nivel de impacto en la disponibilidad del activo cuando se explota una vulnerabilidad con éxito en este activo.

Tareas relacionadas

Configuración de riesgos medioambientales para un activo
Utilice la Puntuación ambiental CVSS para manipular y priorizar la puntuación de riesgo en activos seleccionados. Si configura los parámetros **CVSS, peso y conformidad** para un activo, puede aplicar puntuaciones de riesgo más altas a los activos que son más importantes o críticos.

Investigar puntuaciones de riesgo de vulnerabilidad

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

Mediante IBM 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 no se utiliza para gestionar el riesgo, la columna **Puntuación de riesgo** muestra la puntuación de métrica de entorno CVSS con un valor máximo de 10.

Ajustes de riesgo

Si IBM 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 con QRadar Vulnerability Manager

Tareas relacionadas

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

Clasificación de riesgos personalizada

Utilice puntuaciones de riesgo personalizadas en QRadar Vulnerability Manager para clasificar las vulnerabilidades que representan un mayor riesgo para su organización. La clasificación de riesgos personalizada le permite sustituir un riesgo de vulnerabilidad con su propia clasificación de riesgo.

En función de sus requisitos particulares, es posible que desee sustituir el riesgo de la vulnerabilidad con su propia clasificación de riesgo. Una vulnerabilidad clasificada con una puntuación CVSS alta por QRadar Vulnerability Manager puede no presentar ningún riesgo real debido a muchos factores atenuantes. Por ejemplo si una vulnerabilidad de IPv6 con una puntuación CVSS 9.5 se publica, y una empresa no tiene una infraestructura IPV6, la alta puntuación CVSS no está justificada.

Configuración de puntuaciones de riesgo personalizadas para las vulnerabilidades

En IBM QRadar Vulnerability Manager, puede añadir una puntuación de riesgo personalizada interna a las vulnerabilidades que reflejen el riesgo real para su organización .

Antes de empezar

Nota:

Por la noche, se ejecuta un trabajo de actualización automática para actualizar todos los campos de riesgo personalizados. A efectos de elaboración de informes y de búsquedas guardadas, los cambios en los riesgos personalizados no entran en vigor de manera inmediata. Puede ejecutar la actualización automática de forma manual para rellenar la información sobre los riesgos personalizados que se ha introducido. Para ejecutar la actualización automática, haga clic en el icono **Actualización automática** en la pestaña **Admin**.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Investigar** > **Vulnerabilidades**.
3. Para asignar una puntuación de riesgo personalizada a un activo, lleve a cabo lo siguiente:
   a) Seleccione una vulnerabilidad y haga clic en **Editar/Clasificar**.
   b) Seleccione un tipo de riesgo personalizado en la ventana **Asignación de riesgo personalizado**:

- En blanco: no se ha realizado ningún cambio en el riesgo personalizado, pero se ha asignado una nota.
- Crítico
- Alto
- Medio
- Bajo
- Aviso
- CVSS: la vulnerabilidad tiene un riesgo personalizado establecido de acuerdo con las reglas de la puntuación CVSS actual.
- No asignar: la vulnerabilidad ya no tiene un nivel de riesgo personalizado. Utilice esta opción para eliminar un riesgo personalizado existente.

c) Opcional: Añada una nota utilizando el cuadro de texto RTF para reflejar la asignación de la vulnerabilidad. Por ejemplo, puede añadir una nota para explicar por qué va a cambiar la clasificación.

d) Pulse **Guardar**.

e) Cuando se crea un riesgo personalizado en una vulnerabilidad, se muestra una columna nueva, **Riesgo personalizado**, en la pantalla **Investigar vulnerabilidades**.

4. Para ver los detalles del riesgo personalizado y una nota relacionada con una asignación de riesgo personalizada, haga doble clic en la vulnerabilidad en la pantalla **Investigar vulnerabilidades**.
5. Para buscar vulnerabilidades que no se hayan clasificado todavía, realice los siguientes pasos:
   a) En el panel de navegación, pulse **Investigar** > **Vulnerabilidades**.
   b) Pulse **Buscar** > **Nueva búsqueda**.
   c) En la sección **Nivel de riesgo personalizado**, seleccione uno de los siguientes parámetros de búsqueda:

Tabla 10. Parámetros de búsqueda de riesgos personalizados.

Tipo de búsqueda de riesgo personalizado	Descripción
Todas las vulnerabilidades	Devuelve todas las vulnerabilidades independientemente de si se ha asignado un riesgo personalizado o no.
Todas las vulnerabilidades con clasificación	Devuelve todas las vulnerabilidades con un riesgo personalizado asignado.
Todas las vulnerabilidades que no se han clasificado todavía	Devuelve todas las vulnerabilidades que no tienen un riesgo personalizado asignado.
Todas las vulnerabilidades con el nivel de riesgo personalizado específico	Devuelve vulnerabilidades filtradas en función del tipo de riesgo personalizado que se seleccione; por ejemplo, crítico, alto o intermedio.

   d) Pulse **Buscar**.
6. Exporte una lista de vulnerabilidades desde la pantalla **Lista de vulnerabilidades** a efectos de auditoría o de cumplimiento, realizando lo siguiente:
   a) En el panel de navegación, pulse **Investigar** > **Vulnerabilidades**.
   b) Seleccione la opción de exportación correcta:

- **Exportar a XML**
- **Exportar a CSV**

Buscar datos de vulnerabilidad

En IBM 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) Seleccione un grupo en la lista **Grupo**.
   b) 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. 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 IBM 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 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 11. 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

Parámetros de búsqueda de vulnerabilidades

En IBM 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 12. 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 12. 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 QRadar para sistemas de varios dominios, utilice esta opción para especificar el dominio en el que desea buscar vulnerabilidades.
Por servicio abierto	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	Incluir vulnerabilidades recién publicadas que se detectan en la red y no están presentes en ningún resultado de exploración.
Incluir excepciones de vulnerabilidad	Vulnerabilidades que tienen una regla de excepción aplicada a ellas.

Tabla 12. 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 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	Incluir sólo vulnerabilidades recién publicadas que se detectan en la red y no están presentes en ningún resultado de exploración.
Incluir solo excepciones de vulnerabilidad	Incluir solamente las vulnerabilidades que tienen aplicada una regla de excepción en la búsqueda.
Vencido por días	Buscar vulnerabilidades que están pendientes de corrección y que han vencido hace un número especificado de días.
Estado de parche	Filtrar las vulnerabilidades por estado de parche. Para obtener más información, consulte “Identificar el estado de parche de las vulnerabilidades” en la página 99.
Gravedad de PCI	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	Buscar vulnerabilidades por nivel de riesgo (alto, medio, bajo, aviso).
Sin asignar	Buscar vulnerabilidades sin usuario asignado para que las solucione.
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.

Tabla 12. Parámetros de búsqueda de vulnerabilidades (continuación)	
Opción	**Descripción**
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	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 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. Para incluir la búsqueda guardada en la lista **Búsquedas rápidas** de la barra de herramientas, pulse **Incluir en Búsquedas rápidas**.
7. Para compartir los criterios de búsqueda guardados con todos los usuarios de QRadar, pulse **Compartir con todos**.
8. 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. 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 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 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

Vulnerabilidades de red

En IBM 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 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 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 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. 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

Reducir el número de vulnerabilidades de falso positivo

En IBM 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. 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 13. 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 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

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

En IBM 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 el ejemplo siguiente, 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** > **Nueva**.
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 con QRadar Vulnerability Manager

Tareas relacionadas

Guardar criterios de búsqueda de vulnerabilidades

Configurar colores personalizados para visualizar puntuaciones de riesgo

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

Procedimiento

1. En IBM 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.

   Nota: Los colores que aplica no cambian los colores de riesgo predeterminados en la página **Resultados de exploración**. La columna **Puntuación** de la página **Resultados de exploración** y la página **Resultados de exploración (Detalles de activo)** utiliza valores y colores predeterminados que no puede cambiar.

Identificar vulnerabilidades para las que existe un parche de BigFix

En IBM 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. Ordene las vulnerabilidades de acuerdo con su importancia pulsando la cabecera de columna **Puntuación de riesgo**.
6. Para investigar información sobre parches para una vulnerabilidad, pulse un enlace de vulnerabilidad en la columna **Vulnerabilidad**.
7. 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 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 IBM BigFix

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 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 12. 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

Nota: Una incidencia que se cierra y se vuelve a abrir manualmente muestra un estado de **Reabierto**, que no se puede cerrar mediante una corrección automática. Una incidencia que se ha vuelto a abrir manualmente se debe cerrar manualmente. Si un perfil de exploración detecta una vulnerabilidad que se ha cerrado, el estado de la incidencia se establece en **Abierto**. Estas incidencias se pueden cerrar mediante una corrección automática cuando la vulnerabilidad ya no se detecte en el perfil de exploración.

Tareas relacionadas

Configurar tiempos de corrección para las vulnerabilidades en activos asignados

Asignar vulnerabilidades individuales a un usuario técnico para corregirlas

En IBM 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. 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” en la página 103.
7. 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. 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 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 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. 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. 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. 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. 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 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 13. Informes de vulnerabilidades

En IBM 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 *Guía del usuario de IBM QRadar*.

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 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 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 103.
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 89.

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. 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. 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

Buscar datos de vulnerabilidad

Crear informes de conformidad de PCI

En IBM 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 39.

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

Actualizar declaraciones de planes de conformidad de activos y de software

En IBM 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 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.

Nota:

Algunas columnas de tabla en el documento PDF resultante no se visualizan cuando se crea un informe PDF con los parámetros siguientes:

- Tipo de gráfico - Vulnerabilidades
- Tipo de gráfico - Tabla
- Datos para utilizar - Actuales
- Agrupar por - Instancia

El gran número de columnas de tabla que no caben en una página A4 horizontal estándar hace que se produzca este error.

Para evitar este problema, no utilice la salida en PDF para este tipo de informe. Vea los informes de vulnerabilidades que utilizan Agrupar por Instancia en formato de hoja de cálculo o XML. Para exportar el informe, seleccione **XLS** o **XML** como el formato de informe en el Asistente de informes.

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 14. Exploración de activos nuevos que se comunican con Internet

Utilice IBM QRadar Risk Manager para crear delitos cuando los activos nuevos se comunican con Internet, lo que desencadena una exploración de de los activos por parte de QRadar Vulnerability Manager.

Para desencadenar exploraciones de activos nuevos que se comunican con Internet, siga estos pasos:

1. Cree una búsqueda guardada para activos nuevos.
2. Cree un perfil de exploración bajo demanda con la exploración dinámica habilitada.
3. Cree una pregunta de supervisor de políticas de QRadar Risk Manager destinada a los activos nuevos de la búsqueda guardada de activos.
4. Supervise la pregunta del supervisor de políticas de QRadar Risk Manager.
5. Edite la regla creada por el delito.

Creación de una búsqueda guardada de activos para activos nuevos

Cree una búsqueda guardada para capturar los activos nuevos añadidos a la base de datos dentro del número de días que especifique.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Pulse **Buscar** > **Nueva búsqueda**.
4. Añada los criterios de búsqueda en el panel **Parámetro(s) de búsqueda**.
5. Seleccione **Días desde que se encontró el activo**, **Menor o igual que**, y especifique el número de días.

   Puede especificar otros criterios, pero el criterio más importante es **Días desde que se encontró el activo**.
6. Pulse **Añadir filtro**.
7. Pulse **Buscar**.
8. Pulse **Guardar criterios**.
9. Especifique un nombre para la búsqueda y pulse **Aceptar** para guardar la búsqueda.

Creación de un perfil de exploración bajo demanda

Para desencadenar una exploración en respuesta a un suceso de reglas personalizadas, configure un perfil de exploración bajo demanda y habilite la exploración dinámica.

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**.
4. Añada un **Nombre** y **Direcciones IP** en la pestaña **Detalles**.

   Puede utilizar cualquier dirección IP porque esta dirección IP se sustituye cuando se utiliza la exploración dinámica.
5. Marque el recuadro de selección **Exploración bajo demanda habilitada**

6. Marque el recuadro de selección **Selección de servidor dinámica**.

   Utilice la exploración dinámica en IBM QRadar Vulnerability Manager para asociar exploradores individuales con una dirección IP, rangos de CIDR, rangos de direcciones IP o un dominio que especifique en el perfil de exploración. La exploración dinámica es más útil cuando se despliegan varios exploradores.
7. Pulse **Guardar**.

Conceptos relacionados

Exploraciones de vulnerabilidades dinámicas
En IBM 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.

Detalles de perfil de exploración

Tareas relacionadas

Asociar exploraciones de vulnerabilidades a rangos de CIDR
En IBM 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 IBM QRadar Vulnerability Manager, puede explorar áreas de una red con diferentes exploradores de vulnerabilidades.

Creación de una pregunta de Policy Monitor para probar la comunicación de Internet

Cree una pregunta de QRadar Risk Manager Policy Monitor para probar la comunicación entre activos nuevos e Internet. Los activos nuevos se definen en una búsqueda guardada de activo.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Acciones**, pulse **New Asset Question**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. En la lista **Evaluate On**, seleccione **Actual Communication**.
6. En la lista **Importance Factor**, seleccione el nivel de importancia que desea asociar a esta pregunta.
7. Especifique el rango de tiempo para la pregunta.
8. En el campo **Which tests do you want to include in your question**, seleccione el icono añadir (**+**) junto a las pruebas siguientes:
   - **have accepted communication to the internet**
   - **and include only the following asset saved searches**
9. Configure los parámetros para las pruebas en el campo **Find Assets that**.
   a) Cambie la prueba para **have accepted communication from the internet** pulsando **to**.
   b) Pulse **asset saved searches** y a continuación seleccione la búsqueda guardada.
10. Para asignar la pertenencia a esta pregunta, en el área de grupos, marque los recuadros de selección relevantes.
11. Pulse **Guardar pregunta**.

Supervisión de la comunicación entre activos nuevos e Internet

Configure la pregunta de Policy Monitor para generar un delito cuando un activo de la búsqueda guardada de activo se comunica con Internet.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Seleccione la pregunta que desea supervisar.
4. Pulse **Monitor**.
5. Seleccione un intervalo de **Policy evalutation interval**.
6. Especifique un nombre en el campo **Nombre de suceso**.

   Si selecciona **Asegúrese de que el suceso asignado es parte de un delito**, el *Nombre de suceso* aparece en el campo **Descripción** de un delito cuando selecciona **Todos los delitos** en la pestaña **Delitos**.

   El nombre de la regla generada a partir de un delito es **Risk Question Monitor:** <*Nombre de suceso*>. Este formato de nombre de delito aparece en la pestaña **Delitos** cuando se genera un delito.
7. Especifique una descripción de nombre de suceso.
8. En la sección **Detalles del suceso**, marque el recuadro de selección **Asegúrese de que el suceso asignado es parte de un delito** y **(Correlate By: Asset)** en el menú.
9. En la sección **Additional Actions** :
   - **Correo electrónico**

     Esta opción es útil cuando desea obtener una notificación para el primer suceso enviado como un delito. Puede editar la regla generada a partir de ese delito para desencadenar una exploración. Si no desea recibir notificaciones sobre cada suceso, después de configurar la regla generada por el delito puede desactivar la notificación.
   - **Send to SysLog**

     Si desea registrar el delito, seleccione esta opción.
   - **Notificar**

     Si desea que el suceso aparezca en la alerta de **Notificaciones del sistema** del panel de control, seleccione esta opción.
10. Marque el recuadro de selección **Enable the monitor results function for this question/simulation**.
11. Pulse **Save Monitor**.
12. Pulse **Submit Question**.

Configuración de una regla de delitos para desencadenar una exploración

Para desencadenar una exploración de activos que se comunican con Internet, configure la regla generada por el delito.

Antes de empezar

Se debe generar un delito. Puede generar el delito manualmente o esperar a que un activo se comunique con Internet. Para generar el delito, puede seguir cualquiera de estos pasos:

- Generar un delito manualmente conectando temporalmente cualquier activo nuevo de la búsqueda guardada de activo con Internet.
- Buscar las reglas en la pestaña **Delitos** y buscar la regla una vez generado el delito.

- Habilitar la notificación por correo electrónico para el suceso asignado que crea un delito. Puede editar la regla cuando obtiene esta notificación.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Utilice el recuadro de búsqueda de la barra de herramientas para buscar la regla.

   El nombre de la regla es **Risk Question Monitor:** <*Nombre de suceso*>.

   Puede buscar por el *Nombre de suceso* que es de la ventana **Monitor Question Results**.

   El *Nombre de suceso* de un delito aparece en el campo **Descripción** cuando selecciona **Todos los delitos**.
4. Efectúe una doble pulsación sobre el nombre de regla para abrir el **Asistente de reglas**.
5. Pulse **Siguiente**.
6. Configure los valores siguientes:
   a) Marque el recuadro de selección **Asegúrese de que el suceso detectado es parte de un delito**.
   b) Seleccione **IP de destino** en el menú **Indexar delito según**.
   c) Marque el recuadro de selección **Enviar a SysLog Local**.
   d) Marque el recuadro de selección **Desencadenar exploración**.
   e) Seleccione el perfil de exploración que desea utilizar del menú **Perfil de exploración a utilizar como plantilla**.

      Debe seleccionar la opción **Exploración a petición** en el perfil de exploración que desea utilizar con esta regla.
   f) Pulse el botón de selección **Destino** para el campo **IPs locales a explorar**.
   g) Especifique valores para el valor **Limitador de respuestas**.

      Configure intervalos adecuados para evitar una posible sobrecarga del sistema.
   h) Si no desea acticar esta regla inmediatamente, quite la marca de la opción **Habilitar regla** y a continuación pulse **Finalizar**.

Capítulo 15. Integraciones de software de seguridad

IBM 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 con QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager se integra con IBM 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 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 QRadar Risk Manager User Guide*.

Capítulo 16. Integración de IBM BigFix

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

Por qué utilizar prestaciones de BigFix con la gestión de vulnerabilidades

Anteriormente denominado IBM Security Endpoint Manager, BigFix proporciona visibilidad y control compartidos entre las operaciones de TI y la seguridad. BigFix aplica fixlets a las vulnerabilidades de alta prioridad identificadas y enviadas por QRadar Vulnerability Manager a BigFix. Los fixlets son paquetes que se despliegan en activos o puntos finales para corregir vulnerabilidades específicas. Puede desplegar fixlets simultáneamente en muchos activos o puntos finales desde el panel de control **Gestionar sistemas vulnerables** de la consola de BigFix.

Utilice **Gestionar sistemas vulnerables** de la consola de BigFix para gestionar y controlar una red de cientos de miles de activos o puntos finales en todo un rango de plataformas y dispositivos que se encuentran en cualquier ubicación geográfica.

Cómo remediar vulnerabilidades con BigFix

BigFix proporciona un panel de control que se integra con QRadar Vulnerability Manager. Utilice este panel de control de la consola de BigFix para ver y corregir las vulnerabilidades detectadas y enviadas por QRadar Vulnerability Manager.

Para ver datos de vulnerabilidad de QRadar Vulnerability Manager en la consola de BigFix, configure QRadar Vulnerability Manager y a continuación configure BigFix para procesar los datos de vulnerabilidad enviados desde QRadar Vulnerability Manager. Para obtener información sobre cómo configurar BigFix, consulte el *Manual del usuario de IBM BigFix QRadar*.

Cómo funcionan QRadar Vulnerability Manager y BigFix conjuntamente

QRadar Vulnerability Manager explora los activos o puntos finales para detectar vulnerabilidades y asigna una puntuación de riesgo, que representa el nivel de riesgo que una vulnerabilidad representa para la empresa. QRadar Vulnerability Manager utiliza el parámetro de puntuación de riesgo en el adaptador de BigFix para filtrar las vulnerabilidades de alto riesgo que deben enviarse a BigFix para corregirlas. QRadar Vulnerability Manager asigna un ID de CVE a cada vulnerabilidad que envía a BigFix.

Más información sobre la identificación y el tratamiento de los datos de vulnerabilidad:

La lista siguiente describe el modo en que QRadar Vulnerability Manager y BigFix manejan los datos de vulnerabilidad identificados mediante CVE (Vulnerabilidades y Exposiciones Comunes).

- QRadar Vulnerability Manager envía solamente las vulnerabilidades que tienen ID de CVE a BigFix.
- QRadar Vulnerability Manager envía todos los ID de CVE que están asociados con una única vulnerabilidad a BigFix. Algunas vulnerabilidades pueden tener muchos ID de CVE.
- QRadar Vulnerability Manager sólo envía la CVE con la puntuación de riesgo más alta a BigFix cuando esa CVE muestra dos o más vulnerabilidades.

  Por ejemplo, el ID de CVE siguiente, 2016-0015, muestra dos vulnerabilidades diferentes. Sólo la CVE con la vulnerabilidad de alto riesgo se envía a BigFix.

```
{
Name: CVE-2016-0015
- MS16-007 - Microsoft - DirectShow - Code Execution Issue
Vulnerability ID: 169296
CVE: 2016-0015
Risk: High

Name: Microsoft Windows DirectShow code execution
Vulnerability ID: 169243
CVE: 2016-0015
```

```
Risk: Medium
}
```

BigFix recibe los datos de vulnerabilidad con puntuaciones de riesgo e IDs de CVE de QRadar Vulnerability Manager, que es visible en el panel de control **Gestionar sistemas vulnerables** de BigFix. Utilice el panel de control **Gestionar sistemas vulnerables** de la consola de BigFix para ver y gestionar las vulnerabilidades enviadas por QRadar Vulnerability Manager. BigFix corrige las vulnerabilidades de alto riesgo para las que tiene un Fixlet aplicando un Fixlet directamente al activo o punto final. QRadar Vulnerability Manager recibe una actualización de estado de arreglos de vulnerabilidad de BigFix Web Reports mediante la API SOAP.

Cómo ampliar BigFix a QRadar Risk Manager

Si tiene una instalación de QRadar Risk Manager, puede utilizar políticas de riesgo de QRadar Risk Manager para refinar más las puntuaciones de riesgo de los activos. 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. Puede volver a priorizar las vulnerabilidades que requieren atención inmediata. Si aplica políticas de riesgos a los activos en QRadar Risk Manager, se ajustarán las puntuaciones de riesgo de todas las vulnerabilidades del activo en cuestión. Para obtener más información, consulte la guía del usuario de QRadar Risk Manager.

Corrección de vulnerabilidades

Dependiendo de si ha instalado e integrado BigFix, QRadar Vulnerability Manager proporciona la información siguiente acerca de las vulnerabilidades.

Si BigFix no está instalado

QRadar Vulnerability Manager proporciona actualizaciones diarias sobre las 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.

Utilice la búsqueda de QRadar Vulnerability Manager para 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. QRadar Vulnerability Manager recibe actualizaciones de información de arreglos de vulnerabilidad del servidor de BigFix a intervalos de tiempo preconfigurados.

Utilice la búsqueda de QRadar Vulnerability Manager para identificar las vulnerabilidades cuya corrección está planificada o que ya están corregidas.

Componentes de la integración

Una despliegue integrado típico consta de los componentes siguientes:

- Consola de IBM QRadar.
- QRadar Vulnerability Manager.
- Servidor de BigFix.
- Agente de BigFix en cada destino de exploración de la red.

Tareas relacionadas

Identificar el estado de parche de las vulnerabilidades

Información relacionada

Interacciones entre IBM QRadar e IBM BigFix

Para poder configurar la integración entre IBM QRadar e BigFix, es importante comprender cómo interactúan entre sí.

El diagrama siguiente muestra una visión general de alto nivel de algunas interacciones entre QRadar e BigFix desde la exploración inicial de activos a la remediación de vulnerabilidades en los activos explorados.

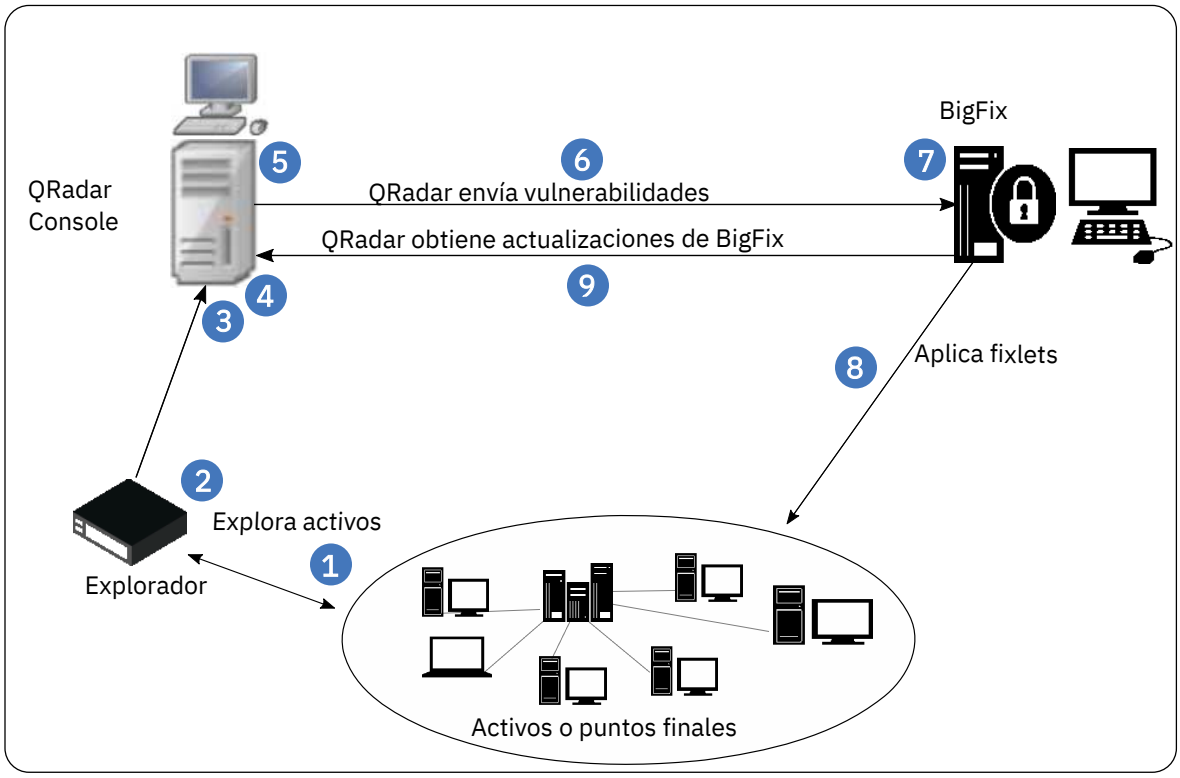

Figura 1. Interacciones entre QRadar Vulnerability Manager e BigFix

La lista siguiente esboza ampliamente las interacciones entre QRadar e BigFix, desde exploración inicial de vulnerabilidades a la remediación de las mismas:

1. El explorador de QRadar Vulnerability Manager realiza una exploración autenticada de activos para descubrir vulnerabilidades. Sólo las vulnerabilidades de activos configurados en perfiles de exploración que utilicen política de exploración Completa, de Parche o PCI son elegibles para el proceso por parte de BigFix.
2. Si un agente de BigFix está instalado en un activo, QRadar Vulnerability Manager recupera el *ID de agente de BES* desde el activo cuando detecta vulnerabilidades en el mismo. El *ID de agente de BES* es el identificador exclusivo utilizado por BigFix para identificar el activo y corregir vulnerabilidades en ese activo. BigFix hace referencia a activos de QRadar como sistemas.
3. Los resultados de la exploración se actualizan en el modelo de activos de QRadar, que incluye el *ID de agente de BES* de cualquier activo que tenga un agente de BigFix. Cuando el estado de la exploración del perfil de exploración muestra un estado de `progress=100%`, el modelo de activos se actualiza y los datos de vulnerabilidad se envían a BigFix en 15 minutos de forma predeterminada.
4. Cuando el modelo de activos se actualiza con los datos de exploración, el adaptador de BigFix que está instalado en QRadar Console recibe los datos de vulnerabilidad actualizados con las puntuaciones de riesgo desde el modelo de activos. Los datos contienen el *ID de agente de BES*. El adaptador de BigFix sólo procesa la información de vulnerabilidad de activos cuando se incluye un *ID de agente de BES*.

5. Los datos de vulnerabilidad que se envían a BigFix se filtran en los parámetros de puntuación de riesgo que están configurados en el archivo de propiedades del adaptador (`/opt/qvm/adaptor/config/adaptor.properties`) de QRadar Console. La puntuación de riesgo predeterminada es 0,0, lo que significa que todas las vulnerabilidades se envían a BigFix.
6. El adaptador de BigFix utiliza la API REST de BigFix para enviar la información de vulnerabilidades a BigFix y correlaciona CVE de vulnerabilidad con fixlets. De forma predeterminada, los datos se envían a BigFix a intervalos de 15 minutos.
7. La información de vulnerabilidad enviada por la API REST API puede visualizarse en el panel de control **Gestionar sistemas vulnerables** de BigFix. Puede desplegar fixlets en los activos con vulnerabilidades de alto riesgo desde el panel de control **Gestionar sistemas vulnerables** de BigFix. BigFix utiliza el *ID de agente de BES* como referencia exclusiva para el activo cuando aplica fixlets directamente al activo.
8. BigFix aplica fixlets a los activos que tienen vulnerabilidades.
9. La API SOAP (Web Reports) se utiliza para obtener el estado de parche de vulnerabilidad desde BigFix. Utilice las búsquedas guardadas y filtros de la pestaña **Vulnerabilidades** para ver esta información de vulnerabilidad actualizada.

   Debe volver a explorar los activos parcheados para actualizar el modelo de activos con el estado de vulnerabilidad revisado de los activos.

Configuración de la comunicación cifrada entre IBM BigFix y QRadar

Para que IBM QRadar Vulnerability Manager reciba actualizaciones de estado de arreglo de vulnerabilidad mediante Web Reports de IBM BigFix, configure TSL (seguridad de la capa de transporte).

Cuando QRadar Vulnerability Manager recibe actualizaciones de estado de Fixlet de BigFix, utiliza la API SOAP para BigFix Web Reports para solicitar actualizaciones mediante consultas que utilizan el lenguaje de relevancia de BigFix. Las consultas se utilizan para extraer datos de la base de datos de BigFix Web Reports que se encuentra en la memoria. QRadar analiza y guarda los datos. Puede utilizar búsquedas guardadas para ver las actualizaciones de BigFix en QRadar. BigFix no utiliza TSL de Web Reports de forma predeterminada. Debe configurar la comunicación TLS y BigFix Web Reports.

Antes de empezar

Los componentes siguientes deben estar instalados en la red:

- Un servidor de BigFix.
- Una consola de BigFix.
- Un agente de BigFix en cada activo de la red que desee explorar.
- Una consola de IBM QRadar.
- Una instalación con licencia de QRadar Vulnerability Manager.

Debe tener QRadar V7.2.6 o posterior con las actualizaciones más recientes.

Nota: Para preparar esta integración, es recomendable ejecutar la **Actualización automática** desde la pestaña **Admin** para obtener las herramientas de exploración más recientes.

Procedimiento

1. Para configurar TLS, siga estos pasos:
   a) Descargue el certificado de clave pública de BigFix en su QRadar Console tecleando el mandato siguiente en el indicador de shell de su QRadar Console.

   ```
   openssl x509 -in <(openssl s_client -connect <dirección IP
   bigfix>:<puerto> -prexit 2>/dev/null) > /opt/qvm/iem/iem_cert.pem
   ```

   Normalmente, BigFix está a la escucha en el puerto 52312.

b) Para crear un almacén de confianza en QRadar, escriba

Especifique el mandato siguiente:

```
keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias
iem_webreports
```

c) Importe el certificado de clave pública de BigFix en el almacén de de confianza de QRadar especificando el mandato siguiente:

```
keytool -importcert -file /opt/qvm/iem/iem_cert.pem -
keystore /opt/qvm/iem/truststore.jks -storepass
<contraseña_almacén_claves> -alias BigFix_webreports
```

d) En el campo de solicitud **¿Confiar en este certificado?**, escriba **Sí**.

2. Para configurar TLS y BigFix Web Reports para QRadar Vulnerability Manager, siga estos pasos:

a) Utilice SSH para iniciar una sesión en la consola de QRadar como usuario root.

b) Especifique `./iem-setup-webreports.pl` y, cuando se le solicite, especifique el nombre de host, puerto de host, nombre de usuario y contraseña del servidor de BigFix.

Puede ejecutar este mandato desde cualquier directorio. Los archivos se crean en el directorio `/opt/qvm/iem`.

c) En el campo de solicitud **¿Utilizar cifrado SSL/TLS?**, escriba la respuesta apropiada.

d) Siga las solicitudes.

e) Para ver el contenido del archivo `webreports.properties`, escriba el mandato siguiente en el indicador de shell:

```
more /opt/qvm/iem/webreports.properties
```

El archivo `webreports.properties` contiene los protocolos de transporte SSL/TLS permitidos, por ejemplo `webreports.tls.protocols=TLSv1.2` o una lista separada por comas `webreports.tls.protocols=TLSv1.2,TLSv1.1`

Verifique que la línea siguiente contiene un número de puerto a continuación de la dirección IP:

```
webreports.endpoint=http://<dirección_IP>:<puerto>/webreports
```

Si desea utilizar un puerto distinto, edite el archivo `/opt/qvm/iem/webreports.properties` y cambie el número de puerto.

Configurar QRadar Vulnerability Manager para enviar datos de vulnerabilidad a BigFix

Instale y configure el adaptador de BigFix en QRadar Console para que IBM QRadar Vulnerability Manager pueda enviar datos de vulnerabilidad con puntuaciones de riesgo a IBM BigFix.

Procedimiento

1. Inicie la sesión en QRadar Console como usuario root.
2. Configure el adaptador de BigFix:

a) Vaya al directorio `/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 almacena el certificado del servidor de BigFix.

El almacén de confianza se crea en `/opt/qvm/adaptor/truststore.jks`

En el directorio `/opt/qvm/adaptor/config` se crean los siguientes archivos de propiedades:

- `adaptor.properties`
- `adaptor-bigfix.properties`

- plugin-bigfix.properties

c) Verifique que el archivo plugin-bigfix.properties tenga una entrada de TLS, por ejemplo TLSv1.2 o una lista de TLS separados por comas TLSv1.2,TLSv1.1,SSLv1.3

La primera entrada de la lista se utiliza para crear el contexto de seguridad: bes.rest.allowed.protocols=TLSv1.2

d) En las solicitudes, proporcione detalles del servidor de la API REST de BigFix especificando el nombre de host o dirección IP, el nombre de usuario y la contraseña para el servidor de BigFix.

El nombre de usuario y la contraseña que especifique son los mismos que las credenciales que se utilizan para la API REST de BigFix. La API REST se utiliza para enviar datos de vulnerabilidad a BigFix.

e) Reinicie el perfilador de activos especificando el mandato siguiente:

```
/opt/qradar/init/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 terceros.

Se crea el archivo adaptor.properties. Este archivo contiene los parámetros de configuración para los datos de vulnerabilidad que se envían a BigFix.

3. Verifique que el proceso de configuración se ha completado satisfactoriamente:

a) En el archivo /opt/qvm/adaptor/config/adaptor.properties, verifique que están establecidas estas propiedades:

```
qvm.adaptor.listener.enabled=true
```

```
qvm.adaptor.process.daemon=false
```

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

Tabla 14. Propiedades de adaptador y descripciones

Nombre de propiedad (API)	**Descripción**
qvm.adaptor.minimum.vuln.riskscore=n	Define el umbral para cada puntuación de riesgo de vulnerabilidad. Esas vulnerabilidades iguales o superiores al valor establecido se envían a BigFix. Por ejemplo, si establece el valor en 5, las vulnerabilidades con puntuaciones de riesgo iguales o superiores a 5 sólo se envían a BigFix.

Tabla 14. Propiedades de adaptador y descripciones (continuación)	
Nombre de propiedad (API)	**Descripción**
qvm.adaptor.minimum.asset.riskscore =n	La puntuación de riesgo acumulado de todas las vulnerabilidades que se encuentran en el activo. Las vulnerabilidades en activos que tienen una puntuación menor que este valor no se envían a BigFix, a menos que el activo tenga vulnerabilidades iguales o superiores al valor establecido para **minimum.vuln.riskscore**. **Nota: minimum.vuln.riskscore** sustituye **minimum.asset.riskscore**. Si **minimum.vuln.riskscore** se establece en 0, todas las vulnerabilidades se envían a IBM BigFix, independientemente del valor de **minimum.asset.riskscore**. Utilice el parámetro **minimum.asset.riskscore** para capturar las vulnerabilidades en activos con vulnerabilidades de bajo riesgo que dan como resultado una puntuación de riesgo acumulado alta para un activo. Cuando establece este valor, debe ser consciente del impacto del valor en **minimum.vuln.riskscore** en este valor.
qvm.adaptor.assetupdate.limit=n	Define cómo se divide el recurso de datos del panel de control de BigFix. La división no se produce hasta que se llenan todos los IDs de CVE para el último activo. • Por ejemplo, **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, **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.source.data.delay=n	Define con qué frecuencia se envían datos a BigFix. Por ejemplo, cuando n=15, se envían datos de vulnerabilidad a BigFix cada 15 minutos, si hay datos de vulnerabilidad disponibles para enviar a BigFix.

Editando el archivo `adaptor.properties`, se filtran los datos de vulnerabilidad que se envían a BigFix.

c) Verifique que la configuración del plug-in BigFix crea los directorios siguientes:

- `/store/qvm/adaptor/data`
- `/store/qvm/adaptor/bigfix`

d) Verifique que el registro está habilitado en el archivo `/opt/qvm/adaptor/log4j.xml`.

Los archivos de registro se encuentran en los archivos `/var/log/qvm-integration-adaptor.log` y `/var/log/qvm-adaptor-cron.log`.

Nota: si no descarga el certificado porque el servidor de BigFix es inaccesible, la configuración no falla. Puede descargar el certificado más adelante ejecutando el mandato siguiente:

`./install-cert.sh` *<ubicación_almacén_confianza> <contraseña_almacén_confianza><dirección_IP_almacén_confianza:puerto>*

Por ejemplo, utilice el formato de mandato siguiente:

```
./install-cert.sh /opt/qvm/adaptor/truststore.jks <abc3password>
<192.0.2.0>:<63455>
```

Resolución de problemas de la integración de BigFix e QRadar Vulnerability Manager

Resolución de los problemas que pueden producirse al configurar la integración de BigFix e QRadar Vulnerability Manager.

Contenido de la resolución de problemas

El certificado de BigFix no se importa debido a una conexión anómala con el servidor de IBM BigFix

Si el certificado no se importa en QRadar debido a una conexión anómala al servidor de BigFix, es posible que vea el siguiente mensaje de error:

```
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 los certificados no están presentes en el almacén de confianza.

Debe cargar manualmente los certificados siguiendo estos pasos cuando tenga acceso al servidor de BigFix.

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.

Verificar la conectividad con IBM BigFix

Para verificar la conectividad con IBM BigFix, siga estos pasos:

1. Escriba el URL siguiente en un navegador web:

   `https://`*`dirección_IP o nombre_host_DNS para BigFix:8080`*`/webreports?page=QNA`

2. Especifique la siguiente serie en una sola línea en el indicador de mandatos:

   ```
   (id of site of it,id of it,name of it,cve id list of it) of fixlets whose
   (cve id list of it as lowercase contains "cve") of bes sites
   ```

3. Pulse **Evaluar**

La serie siguiente es un ejemplo de la salida de un resultado:

```
2, 104301, MS01-043: NNTP Service in Windows NT 4.0
Contains Memory Leak, CVE-2001-0543
```

La tabla siguiente describe el desglose de este resultado:

Tabla 15. Resultado de la consulta

Resultado	**Parámetro de consulta**	**Descripción**
2	(id of site of it)	ID de sitio de Fixlet
104301	(id of it)	ID de Fixlet
MS01-043: NNTP Service in Windows NT 4.0 Contains Memory Leak	(name of it)	Nombre de Fixlet
CVE-2001-0543	(cve id list of it)	ID de CVE

¿Están instaladas las herramientas de exploración más recientes?

Debe ejecutar actualizaciones automáticas para obtener las herramientas de exploración más recientes para las instalaciones nuevas de QRadar, ya que son necesarias para que esta integración funcione. Ejecute la actualización automática desde la pestaña **Admin** pulsando el icono **Actualización automática**.

Para obtener más información sobre la instalación de actualizaciones automáticas de QRadar, consulte la *Guía de administración de IBM QRadar*.

¿Está instalada la característica de exploración de BigFix?

Ejecute el mandato siguiente para comprobar si la característica de exploración de BigFix está instalada en QRadar:

```
grep -rl 'BIG_FIX_AGENT_ID' /opt/qvm
```

Si la característica de exploración de BigFix está instalada, se devuelven los resultados siguientes:

- `/opt/qvm/sys/perl/scanner/FusionVM/smb_patch_scanning.pm`
- `/opt/qvm/bin/ssh/packages/bin/ssh-packages`

Si no ve estos archivos, ejecute la actualización automática desde la pestaña **Admin** pulsando el icono **Actualización automática**.

Restablecimiento de contraseñas

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

1. Edite el archivo `plugin-bigfix.properties` que se encuentra en el directorio `/opt/qvm/adaptor/config`.
2. Sustituya la línea siguiente:

`_decrypt.bes.rest.password=lUb5qzr7FIVH+J319erc+g==`

por la línea siguiente:

`_encrypt.bes.rest.password=newpassword`

donde `newpassword` es la contraseña nueva.

3. Ejecute el script siguiente para cifrar la contraseña nueva:

   `./password-property-encrypt.sh plugin-bigfix.properties`

Error de excepción de contraseña en el archivo /var/log/iem-cron.log

Puede ver el error siguiente en el archivo `/var/log/iem-cron.log`.

```
Exception in thread "main" java.lang.NoClassDefFoundError:
com.sun.org.apache.xerces.internal.dom.ElementNSImpl
```

Este error de excepción de contraseña se produce cuando el archivo `/opt/qvm/iem/webreports.properties` utiliza una contraseña no válida.

Para arreglar este error, en el indicador de shell, ejecute `/opt/qvm/iem/iem-setup-webreports.pl` y vuelva a especificar la contraseña correcta.

Los datos de exploración de vulnerabilidades no se envían a BigFix

Verifique que el explorador puede autenticarse en el activo y acceder a la información necesaria.

1. Pulse la pestaña **Vulnerabilidades**.
2. En la fila de nombre de exploración, pulse el número de la columna **Activos**.
3. Pase el ratón sobre los símbolos de aviso que aparecen en la columna con el icono de distintivo.
4. Compruebe si existen problemas de credenciales en el perfil de exploración o problemas de configuración de activos que impidan que el explorador acceda a la información necesaria.

¿Está actualizado el modelo de activos?

Para verificar que el modelo de activos se actualiza con los resultados de exploración:

1. Pulse la pestaña **Vulnerabilidades**.
2. En el menú de navegación, pulse **Resultados de exploración**.

   Si ve un triángulo de aviso rojo, el modelo de activos no se ha actualizado con los resultados de exploración.

Inhabilitación de la integración de BigFix e QRadar Vulnerability Manager

Utilice el procedimiento siguiente si desea inhabilitar la integración de BigFix y QRadar Vulnerability Manager.

Procedimiento

1. Inicie la sesión en QRadar Console como usuario root.
2. Para inhabilitar el adaptador de QRadar Vulnerability Manager escriba los mandatos siguientes:
   - `systemctl stop qvmadaptor.timer`
   - `systemctl disable qvmadaptor.timer`
   - `systemctl daemon-reload`
3. Escriba el mandato siguiente para cambiar el nombre del directorio `/store/qvm/adaptor`:
   `mv /store/qvm/adaptor /store/BigFix.old/`

4. Escriba el mandato siguiente para reiniciar el perfilado de activos:
   `systemctl restart assetprofiler`

   Consejo: Si en otro momento desea volver a habilitar la integración de BigFix, puede invertir el proceso indicado más arriba.

Capítulo 17. 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 de QRadar Vulnerability Manager se reenvían automáticamente a SiteProtector.

QRadar Vulnerability Manager reenvía las vulnerabilidades de los resultados de exploración que están etiquetadas con IDs de ISS X-Force de IBM Security SiteProtector. QRadar Vulnerability Manager utiliza el agente de MSL para reenviar las vulnerabilidades.

Conexión con IBM Security SiteProtector

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

Procedimiento

1. En el menú de navegación (☰), pulse **Admin**.
2. Haga clic en **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar despliegue de vulnerabilidades**.
3. Pulse **Utilizar SiteProtector**.
4. En el campo **Dirección IP de SiteProtector**, escriba la dirección IP del servidor de IBM Security SiteProtector Agent Manager.

   El puerto predeterminado para esta conexión es 3995.
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**.

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 18. Investigación, noticias y avisos sobre vulnerabilidades

Puede utilizar IBM 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 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. Si no se visualiza ninguna vulnerabilidad, seleccione un rango de tiempo alternativo en la lista **Ver vulnerabilidades desde**.
4. 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 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 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 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.

Capítulo 19. IBM QRadar Vulnerability Manager Engine para las pruebas de vulnerabilidad de red (NVT) de OpenVAS

El producto IBM QRadar Vulnerability Manager (QVM) Engine para las pruebas de vulnerabilidad de red de OpenVAS implementa la política de exploración completa plus que incorpora una dimensión de más profundidad a la exploración sin credenciales.

Acerca de QVM Engine para NVT de OpenVAS

El proyecto de código abierto OpenVAS proporciona alrededor de 50.000 NVT (pruebas de vulnerabilidad de red) individuales a través de su canal de información de comunidad. Estas NVT son pruebas individuales que pueden evaluar una vulnerabilidad. El producto QVM Engine para NVT de OpenVAS proporciona la posibilidad de ejecutar estas pruebas como parte de una exploración de QVM.

Características

El producto QVM Engine para NVT de OpenVAS instala una nueva política de exploración denominada política de exploración completa plus, independiente de las políticas de exploración existentes. Puesto que contiene más pruebas de vulnerabilidad, se necesita más tiempo para llevar a cabo las exploraciones. Las exploraciones configuradas anteriormente utilizan las redes de Opencast además de las prestaciones de QRadar Vulnerability Manager.

La política de exploración completa plus incluye miles de pruebas de vulnerabilidad adicionales que proporciona el proyecto de OpenVAS.

Las NVT se actualizan de noche a través de las actualizaciones automáticas existentes. No es necesaria ninguna configuración adicional.

Requisitos

El producto QVM Engine para NVT de OpenVAS requiere la versión 7.3.1 con el parche 3, o posterior de QRadar con una licencia de QRadar Vulnerability Manager.

La instalación requiere actualizaciones automáticas y acceso a la consola. Consulte “Adición de la política de exploración completa plus a IBM QRadar Vulnerability Manager” en la página 136.

Preguntas más frecuentes

¿El producto QVM Engine para NVT de OpenVAS permite importar vulnerabilidades en QRadar Vulnerability Manager desde un despliegue autónomo de OpenVAS?

No. Este plug-in permite que QVM ejecute pruebas de vulnerabilidad de red de OpenVAS como parte de las exploraciones de QVM pero no se ha diseñado para proporcionar a la integración una instancia independiente de OpenVAS.

¿La política de exploración completa plus se ejecuta solamente en NVT de OpenVAS?

No. La política de exploración completa plus utiliza una combinación de pruebas de exploración de QVM con las NVT para ofrecer mayor cobertura.

Acerca de la política de exploración completa plus

La política de exploración completa plus ejecuta OpenVAS NVT, así como las herramientas de la política de exploración completa existentes. Como consecuencia, la detección de vulnerabilidad se mejora allí

donde son necesarias las exploraciones sin autenticar y el tiempo permite ejecutar esas pruebas adicionales.

Nota: Debe instalar el RPM de política de exploración completa plus para utilizar esta política de exploración.

La política de exploración completa plus utiliza un canal de información que se actualiza diariamente de alrededor de 50.000 NVT (Network Vulnerability Tests - pruebas de vulnerabilidad de red) individuales que proporciona el proyecto de código abierto de OpenVAS.

De forma predeterminada, la política detecta los activos de red utilizando un rango de puertos de exploración rápida (FAST). Se ejecuta una exploración autenticada cuando se proporcionan credenciales.

Una exploración completa consta de las fases siguientes:

Tipo de exploración	Descripción
Exploración de descubrimiento.	Descubre activos de red y luego explora los puertos para identificar las características de activos clave, como por ejemplo sistema operativo, tipo de dispositivo y los servicios. Las vulnerabilidades no se exploran.
Exploración 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. **Nota:** La característica más potente de la política de exploración completa plus es su exploración sin credenciales completa, que ejecuta más pruebas que la exploración completa, que se proporcionan mediante la comunidad de código abierto. Esta exploración es más detallada que la exploración completa pero tarda más y utiliza más recursos. Ejecute esta exploración durante periodos de inactividad en la red, lo ideal es por la noche o durante el fin de semana.
Exploración con credenciales	QRadar Vulnerability Manager registra la información en el activo y recopila información acerca del inventario de aplicaciones instaladas y la configuración necesaria; también genera o suprime vulnerabilidades.

Adición de la política de exploración completa plus a IBM QRadar Vulnerability Manager

Para añadir la política de exploración completa plus a IBM QRadar Vulnerability Manager, debe descargar el producto QVM Engine para RPM de NVT de OpenVAS desde IBM® Fix Central e instalarlo en la consola de IBM QRadar.

Antes de empezar

- Asegúrese de que tiene instalada la versión 7.3.1, parche 3, o posterior, de QRadar.
- Asegúrese de que el procesador y el escáner de QRadar Vulnerability Manager estén habilitados.

Procedimiento

1. Descargue el RPM de IBM Fix Central y guárdelo en el directorio `/store/rpms` de la consola.
2. Escriba el mandato siguiente para instalar el RPM en la consola de QRadar.
   ```
   rpm -ivh /store/rpms/qvm-openvas-x.x-x.noarch.rpm
   ```
   Nota: En un entorno de alta disponibilidad, lleve a cabo este paso solamente en la consola principal.
3. Escriba el mandato siguiente para habilitar la política de exploración completa plus:
   ```
   /store/qvm/openvas/openvas_switch.sh enable
   ```

Nota: Lleve a cabo este paso solamente en la consola. Este paso despliega la configuración en todo el sistema. No es necesario llevar a cabo ninguna acción en los host gestionados.

4. Ejecute las actualizaciones automáticas llevando a cabo las tareas siguientes:

   a) En el menú de navegación (☰), pulse **Admin**. para abrir la pestaña de administración.

   b) En la sección **Configuración del sistema**, pulse **Actualización automática**.

   c) Pulse **Obtener nuevas actualizaciones**.

   d) Si aparecen actualizaciones nuevas en la lista, pulse **Instalar** > **Todas las actualizaciones**.

   Importante: Debe activar la actualización automática para llevar a cabo la instalación de la política de exploración completa plus. En este momento, se descargan y se instalan herramientas adicionales. La política de exploración estará disponibles en la interfaz de usuario una vez finalizada la instalación. Debe llevar a cabo este paso, incluso si ya se ha ejecutado la actualización automática en el día actual.

Ejecución de una exploración

Lleve a cabo los pasos siguientes para ejecutar una exploración con la política de exploración completa plus.

Procedimiento

1. Configure la nueva política de exploración completa plus según sea necesario.

   Para obtener instrucciones sobre cómo configurar una política de exploración, consulte la información siguiente.

2. Cree un perfil de exploración y seleccione **Política de exploración completa plus** o la política que haya creado en el Paso 1 en el menú **Políticas de exploración**.

   Para obtener instrucciones sobre cómo crear una política de exploración, consulte la información siguiente.

Configuración de una política de exploración

En IBM QRadar Vulnerability Manager,puede configurar una política de exploración para ajustarse a los requisitos específicos de sus exploraciones de vulnerabilidad. Puede copiar y renombrar una política de exploración preconfigurada o puede añadir una política de exploración nueva. No puede editar una política de exploración preconfigurada.

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, debe configurar como mínimo los campos obligatorios de la ventana **Política de exploración nueva** que son **Nombre** y **Descripción**.

5. En la lista **Tipo de exploración** seleccione el tipo de exploración.
6. Para gestionar y optimizar el proceso de descubrimiento de activos, pulse la pestaña **Descubrimiento de activos**.
7. Para gestionar los puertos y protocolos que se utilizan para una exploración, pulse la pestaña **Exploración de puertos**.
8. Para incluir vulnerabilidades específicas en la política de exploración de parches, pulse la pestaña **Vulnerabilidades**.

Nota: La pestaña **Vulnerabilidades** solo está disponible cuando selecciona una exploración de parches.

9. Para incluir o excluir grupos de herramientas de la política de exploración, pulse la pestaña **Grupos de herramientas**.

   Nota: La pestaña **Grupos de herramientas** sólo está disponible cuando se selecciona una política de exploración completa plus o de exploración completa de cero credenciales.

10. Para incluir o excluir herramientas de una política de exploración, pulse la pestaña **Herramientas**.

    Nota: La pestaña **Herramientas** sólo está disponible cuando se selecciona una política de exploración completa plus o de exploración completa de cero credenciales.

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

11. Pulse **Guardar**.

Crear un perfil de exploración

En IBM 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 *Guía de administración de IBM QRadar*.

4. Pulse **Guardar**.

Conceptos relacionados

Ancho de banda de red para exploraciones de activos simultáneas

Ajustando el valor de ancho de banda de red, cambiará el número de activos que se pueden explorar simultáneamente y el número de herramientas de vulnerabilidad que pueden utilizarse simultáneamente para explorar los activos. Algunas exploraciones utilizan más herramientas de vulnerabilidad para la exploración, lo cual afecta al número de activos que se pueden explorar simultáneamente.

Exploración dinámica

Utilice la exploración dinámica en IBM QRadar Vulnerability Manager para asociar exploradores individuales con una dirección IP, rangos de CIDR, rangos de direcciones IP o un dominio que especifique en el perfil de exploración. La exploración dinámica es más útil cuando se despliegan varios exploradores. Por ejemplo, si despliega más de 5 exploradores, puede ahorrar tiempo utilizando la exploración dinámica.

Opciones para añadir exploradores al despliegue de QRadar Vulnerability Manager

Políticas de exploración

Exploraciones de vulnerabilidades dinámicas

En IBM 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 IBM 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

Configuración de una política de exploración

En IBM QRadar Vulnerability Manager,puede configurar una política de exploración para ajustarse a los requisitos específicos de sus exploraciones de vulnerabilidad. Puede copiar y renombrar una política de exploración preconfigurada o puede añadir una política de exploración nueva. No puede editar una política de exploración preconfigurada.

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

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 contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de 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.

Cualquier referencia hecha en esta publicación a sitios web que no pertenecen a IBM se proporciona sólo por comodidad del usuario y de ninguna forma supone la promoción de esos sitios web. Los materiales de estos sitios web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios web es de la entera 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119

Armonk, NY 10504-1785
US

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 ejemplos de datos de rendimiento y de clientes mencionados se incluyen sólo por razones ilustrativas. Los resultados de rendimiento reales pueden variar dependiendo de las configuraciones y condiciones operativas específicas.

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.

Las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente 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 y cualquier parecido con nombres reales de personas y empresas es pura coincidencia.

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.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o de sus filiales.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

Términos y condiciones de la documentación de producto

Los permisos para utilizar estas publicaciones se otorgan de acuerdo con los términos y condiciones siguientes.

Ámbito de aplicación

Estos términos y condiciones se añaden a los términos de uso del sitio web de IBM.

Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre que se conserven todos los avisos sobre derechos de propiedad. El usuario no puede distribuir, mostrar ni realizar trabajos derivados de estas publicaciones, ni de ninguna parte de las mismas, sin el consentimiento explícito de IBM.

Uso comercial

El usuario puede reproducir, distribuir y visualizar estas Publicaciones exclusivamente dentro de la empresa siempre y cuando se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni de partes de las mismas, ni reproducirlas, distribuirlas o visualizarlas fuera de la empresa sin el consentimiento expreso de IBM.

Derechos

A excepción de lo especificado expresamente en este permiso, no se concede ningún otro permiso, licencia o derecho, ni explícito ni implícito, para la información o los datos, el software ni ninguna otra propiedad intelectual que contenga.

IBM se reserva el derecho de retirar los permisos que se hayan proporcionado siempre que, bajo su discreción, el uso de las publicaciones sea perjudicial para sus intereses o, según determine IBM, no se estén siguiendo adecuadamente las instrucciones detalladas anteriormente.

No puede descargar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, NO VULNERACIÓN DE DERECHOS Y ADECUACIÓN PARA UN FIN DETERMINADO.

Declaración de privacidad en línea de IBM

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.

Reglamento general de protección de datos

Los clientes son responsables de garantizar que cumplen diversas normativas y leyes, incluido el Reglamento general de protección de datos de la Unión Europea. Los clientes son los únicos responsables de obtener asesoramiento legal competente respecto a la identificación y la interpretación de cualquier normativa y ley que pueda afectar a los negocios de los clientes y a cualquier acción que los clientes puedan deber emprender para cumplir con dichas normativas y leyes. Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetos a disponibilidad. IBM no proporciona asesoramiento legal, contable ni de auditoría, ni garantiza que sus servicios o productos vayan a garantizar que los clientes cumplan cualquier normativa o ley.

Puede obtener más información sobre la preparación para el cumplimiento del Reglamento general de protección de datos de IBM, así como de nuestras prestaciones y ofertas en relación con el Reglamento general de protección de datos aquí: https://ibm.com/gdpr

Glosario

Este glosario proporciona términos y definiciones para el software y productos de IBM 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 terminología de IBM (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

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

Z