Guía del usuario de Nessus Perimeter Service (interfaz HTML5)

16 de enero de 2014

(Revisión 5)

Índice

Introducción 3

Nessus Perimeter Service 3

Suscripción y activación 3

Interfaz de análisis del cliente 4

Directivas de análisis 5

Creación e inicio de un análisis 6

Programación de un análisis 7

Administración de análisis 8

Visualización de los resultados de un análisis 8

Revisión de los resultados de un análisis 9

Validación de ASV de PCI 11

Envío de resultados de análisis para la revisión del cliente de PCI 12

Interfaz de revisión del cliente 13

Revisión de los resultados de un análisis 14

Cuestionamiento de los resultados de un análisis 16

Envío de adjuntos como evidencia para un cuestionamiento 19

Envío de un informe de análisis para la revisión de Tenable 21

Formatos de informe ASV de PCI 24

Soporte 27

Cambio de la contraseña 27

Para obtener más información 27

Acerca de Tenable Network Security 28

Introducción

Este documento describe el Nessus Perimeter Service de Tenable Network Security. Envíe sus comentarios o sugerencias por correo electrónico a support@tenable.com.

En este documento se trata el Nessus Perimeter Service según su aplicación para el análisis, la evaluación y la generación de informes de vulnerabilidades. El contenido de este documento comprende los procesos de la suscripción y activación al Perimeter Service, la iniciación de análisis de clientes, la generación de informes de vulnerabilidades y compatibilidad, la validación de ASV de PCI y el soporte del Perimeter Service. El Nessus Perimeter Service se ofrece con las interfaces Flash y HTML5. En este documento se describe la interfaz HTML5. Si está utilizando la interfaz Flash, que es la opción predeterminada solo para el explorador Microsoft Internet Explorer, consulte el documento “Nessus Perimeter Service User Guide (Flash Interface)” (Guía del usuario de Nessus Perimeter Service [interfaz Flash]) disponible en el Tenable Support Portal (Portal de soporte de Tenable).

Se presupone un conocimiento básico del analizador de vulnerabilidades Nessus de Tenable, protocolos de red, análisis y corrección de vulnerabilidades, y servicios en la nube.

Las consideraciones y notas importantes se resaltan con este símbolo y cuadros de texto grises.

Las sugerencias, los ejemplos y las prácticas recomendadas se resaltan con este símbolo y con letras blancas en cuadros de texto azules.

Nessus Perimeter Service

El Nessus Perimeter Service es un servicio de análisis de vulnerabilidades remoto para empresas que puede ser utilizado para auditar direcciones IP con conexión a Internet en busca de vulnerabilidades en redes y en aplicaciones web “desde la nube”. Los suscriptores, que tienen acceso a los analizadores de Nessus alojados en el centro de datos seguro de Tenable, pueden utilizar el Nessus Perimeter Service para analizar cualquier cantidad de sitios con conexión a Internet en una amplia variedad de dispositivos: servidores de empresas, computadoras de escritorio, computadoras portátiles, teléfonos iPhone, etc., donde sea conveniente y con la frecuencia necesaria. Todo por una tarifa plana.

El portal del Nessus Perimeter Service ofrece un acceso seguro a las detalladas auditorías de vulnerabilidades e informaciones de corrección alojadas en la infraestructura de Tenable. Puede acceder al Nessus Perimeter Service desde cualquier computadora con acceso a Internet y un explorador web estándar, así como también desde dispositivos móviles como teléfonos con Android y teléfonos iPhone o dispositivos iPad. Esto le proporciona un comando y control fijo o móvil del analizador y acceso a informes de vulnerabilidades y compatibilidad desde cualquier lugar, en cualquier momento. El soporte del Nessus Perimeter Service está a cargo de un equipo de investigación de reputación internacional, que cuenta con la base de conocimiento en vulnerabilidades más grande de la industria, lo que lo hace ideal incluso para las auditorías más complejas.

Suscripción y activación

El Nessus Perimeter Service de Tenable está disponible a través de una suscripción anual. Puede obtener las suscripciones en la Tenable Store (Tienda de Tenable). Para obtener información sobre los precios, visite la Tienda de Tenable o envíe su consulta a subscriptions@tenable.com para obtener más información.

Un paquete de suscripción al Nessus Perimeter Service comprende:

- Análisis ilimitado de los sistemas de su perímetro
- Auditorías de aplicaciones web
- Capacidad para elaborar evaluaciones de seguridad según los estándares PCI actuales

- Hasta 2 envíos de informes trimestrales para la validación de ASV de PCI a través de Tenable Network Security, Inc.
- Acceso en todo momento al Tenable Support Portal (Portal de soporte de Tenable) para consultar la base de conocimiento de Nessus y crear tickets de soporte
- Una cuenta de usuario por suscripción

Al comprar una suscripción al Nessus Perimeter Service, Tenable Product Delivery (Entrega de productos de Tenable) notificará al cliente por correo electrónico la disponibilidad del producto. El correo electrónico de notificación también incluirá el número de pedido del cliente, la fecha de vencimiento del producto y un enlace de activación del producto. Puede consultar en línea un documento de ayuda de activación en:

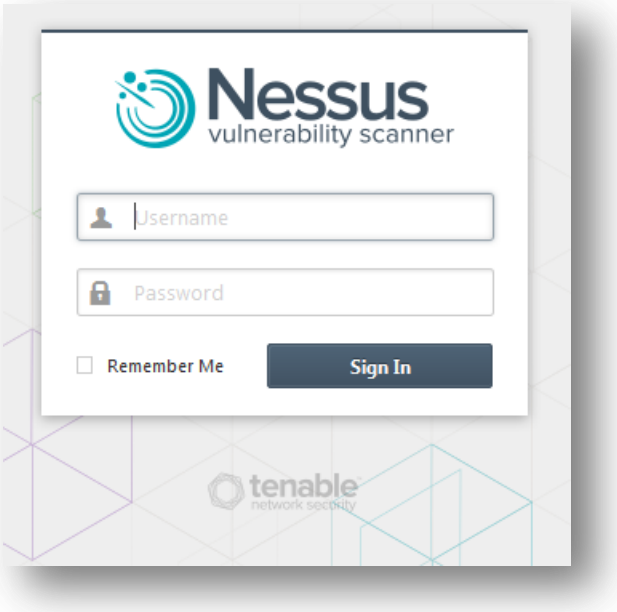
http://static.tenable.com/documentation/PS_Activation_Help.pdf

Si tiene algún problema con el proceso de activación, contáctese con licenses@tenable.com. Debe incluir su Customer ID (Identificación de cliente) en cualquier consulta. Si no tiene Identificación de cliente, indique el número de pedido para recibir la asistencia adecuada.

Interfaz de análisis del cliente

Los clientes que se suscriben al Nessus Perimeter Service interactúan con un portal web seguro. Para acceder al servicio, todos los clientes necesitan credenciales para el portal que son proporcionadas por Tenable Network Security en el momento de la compra del servicio.

La siguiente captura de pantalla muestra la página de inicio de sesión del portal, que ofrece la interfaz del usuario de Nessus en HTML5 de manera predeterminada:



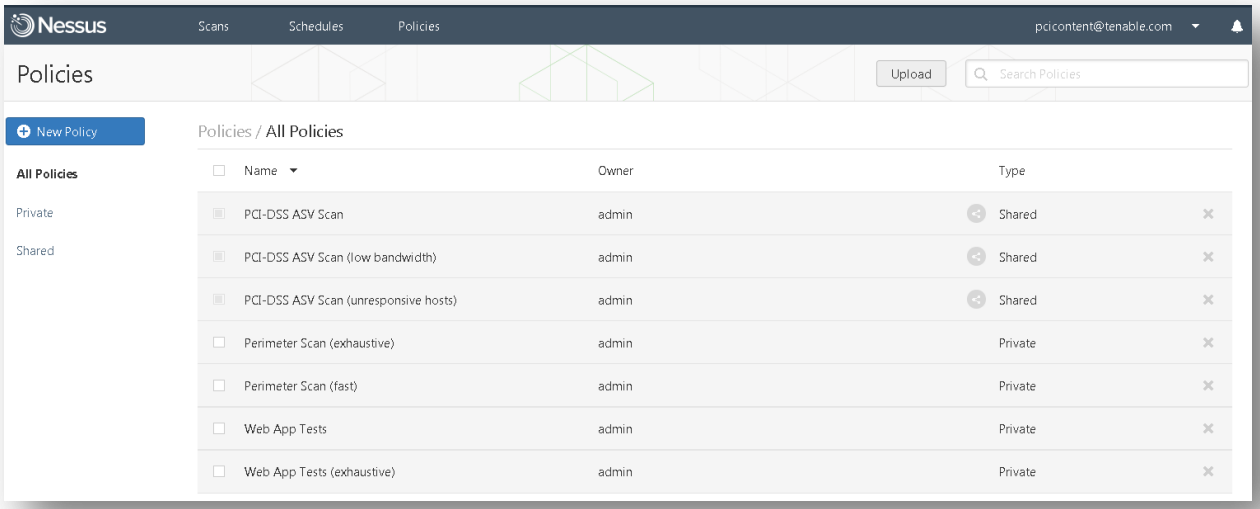
Pantalla de inicio de sesión del Nessus Perimeter Service

Para obtener más información sobre cómo usar el Nessus Perimeter Service con la interfaz Flash más antigua, consulte el documento “Nessus Perimeter Service User Guide (Flash Interface)” (Guía del usuario de Nessus Perimeter Service [interfaz Flash]) disponible en el Tenable Support Portal (Portal de soporte de Tenable).

Directivas de análisis

Una vez que inician sesión en el servicio, los clientes de Nessus Perimeter Service tienen la opción de seleccionar una de siete directivas de análisis predeterminadas:

- Perimeter Scan (exhaustive) (Análisis de perímetro [exhaustivo]): esta directiva utilizará más ancho de banda pero encontrará todos los servicios TCP externos alojados en una red con conexión externa. Esta directiva contiene la configuración predeterminada que ejecutará un análisis de perímetro exhaustivo:
  - Un análisis de puertos rápido que verifica 65 536 puertos TCP
  - Las comprobaciones de CGI están habilitadas
  - Las comprobaciones de aplicaciones web están deshabilitadas
  - Baja proporción de falsos positivos
- Perimeter Scan (fast) (Análisis de perímetro [rápido]): esta es una directiva ideal para ejecutar como análisis inicial. Esta directiva contiene la configuración predeterminada que ejecutará un análisis de perímetro rápido:
  - Un análisis de puertos rápido que verifica los 8000 puertos TCP más comunes
  - Las comprobaciones de CGI están habilitadas
  - Las comprobaciones de aplicaciones web están deshabilitadas
  - Baja proporción de falsos positivos
- Web App Tests (exhaustive) (Pruebas de aplicaciones web [exhaustivas]): esta directiva ejecutará una prueba de aplicaciones web en el host remoto. Se buscarán vulnerabilidades personalizadas en las aplicaciones, se utilizará el método “todos los pares” para la prueba de argumentos, se comprobarán todos los parámetros de cada página y se ejecutará durante 24 horas como máximo.
- Web App Tests (fast) (Pruebas de aplicaciones web [rápidas]): esta directiva ejecutará una prueba de aplicaciones web en el host remoto. Se buscarán vulnerabilidades personalizadas en las aplicaciones, se utilizará el método “todos los pares” para la prueba de argumentos, se comprobarán todos los parámetros de cada página y se ejecutará durante 2 horas como máximo.
- PCI-DSS ASV Scan (Análisis ASV de PCI-DSS): pueden utilizar esta directiva los clientes del Perimeter Service que deseen ejecutar análisis de vulnerabilidades externas que puedan utilizarse en tareas de validación de compatibilidad PCI DSS. Puede encontrar más información acerca de la ejecución de análisis con la directiva ASV de PCI DSS y la validación de análisis a través del servicio ASV de PCI de Tenable más adelante en este documento.
- PCI-DSS ASV Scan (low bandwidth) (Análisis ASV de PCI-DSS [ancho de banda bajo]): esta directiva es idéntica a la directiva de análisis ASV de PCI DSS con la excepción de la opción “max_hosts”, que está establecida en “2” para limitar la cantidad de ancho de banda utilizada por los análisis de Nessus Perimeter Service.
- PCI-DSS ASV Scan (unresponsive hosts) (Análisis ASV de PCI-DSS [los hosts no responden]): esta directiva es idéntica a la directiva de análisis ASV de PCI DSS con la excepción de la opción “Ping Host” (Efectuar pings a host), que está deshabilitada para permitir que los análisis del Nessus Perimeter Service pasen a diferentes opciones de análisis en lugar de dejar de analizar un host porque el host no responda a un ping remoto.



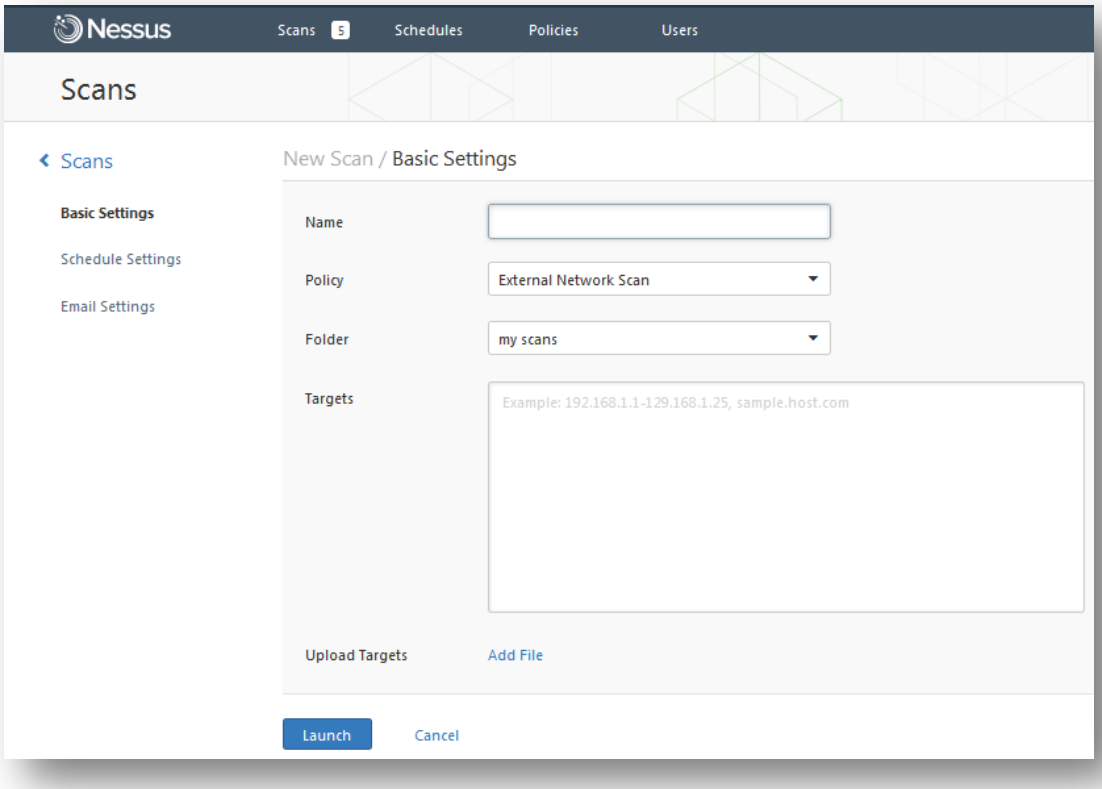
El personal de Tenable revisa y actualiza periódicamente estas directivas para garantizar que incluyan actualizaciones para familias de plugins y otras mejoras a la configuración. Los clientes no tienen la capacidad de ver ni alterar ninguno de los parámetros preestablecidos de la directiva PCI DSS.

En lugar de editar directamente las directivas de análisis preestablecidas, se recomienda especialmente hacer una copia de una directiva de análisis preestablecida y editar la copia. Si editó directamente una directiva de análisis preestablecida, la autoría de la directiva cambiará de “admin” al usuario del Nessus Perimeter Service y no podrá restaurar automáticamente la configuración original.

El botón “**Upload**” (Cargar) le permitirá cargar en el analizador del Perimeter Service las directivas creadas con anterioridad. Mediante el cuadro de diálogo “**Browse…**” (Explorar), seleccione la directiva de su sistema local y haga clic en “**Submit**” (Enviar).

Creación e inicio de un análisis

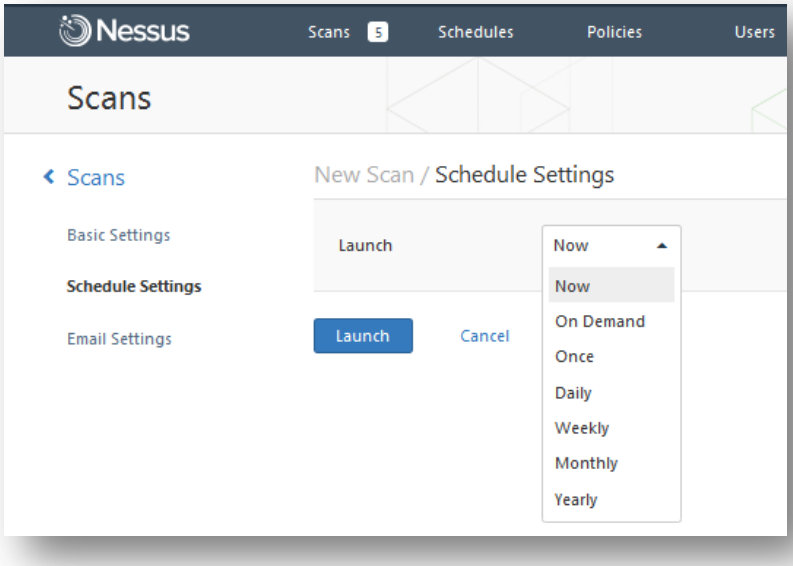
Para crear un análisis, un cliente del Nessus Perimeter Service ingresa en la sección “**Scans**” (Análisis) y selecciona “New Scan” (Nuevo análisis). Luego introduce un nombre exclusivo para el análisis y el tipo de análisis, selecciona la directiva e introduce la o las direcciones IP, el o los rangos de IP, o los nombres de host de sus servidores con conexión externa que serán el destino del análisis.



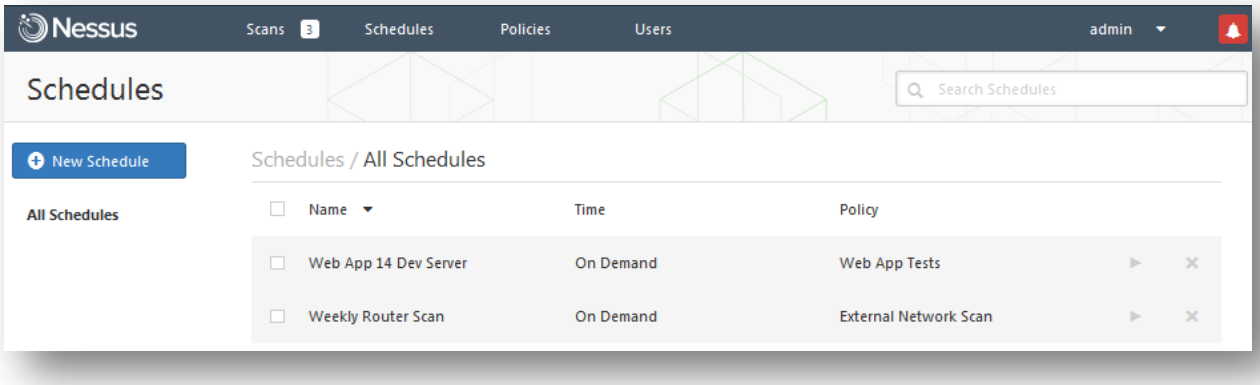
Haga clic en "**Launch**" (Iniciar) para iniciar el nuevo análisis de inmediato.

Programación de un análisis

Para iniciar un análisis como plantilla, primero cree un nuevo análisis por medio del menú "**Scans**" (Análisis) o "**Schedules**" (Programas). Después de completar la configuración básica, escoja "**Schedule Settings**" (Configuración del programa) y la frecuencia:

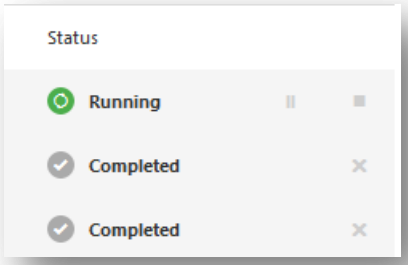


Una vez que lo guardó, puede acceder a los análisis programados por medio del menú “**Schedules**” (Programas) en la parte superior:



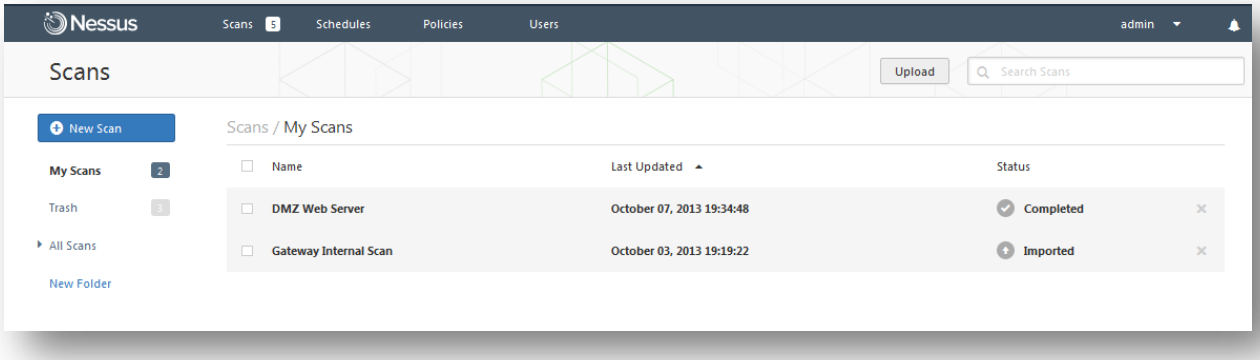
Administración de análisis

Una vez que se iniciaron, los análisis pueden pausarse o detenerse durante el proceso de análisis mediante el uso del ícono de pausa o interrupción a la derecha del análisis:



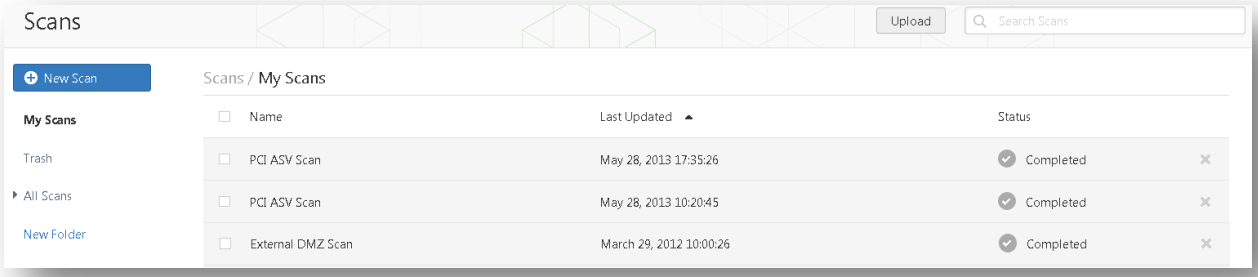
Visualización de los resultados de un análisis

Puede ver los resultados obtenidos en un análisis actualmente en curso seleccionando el menú “**Scans**” (Análisis) y haciendo clic en el análisis que está en ejecución o completado:

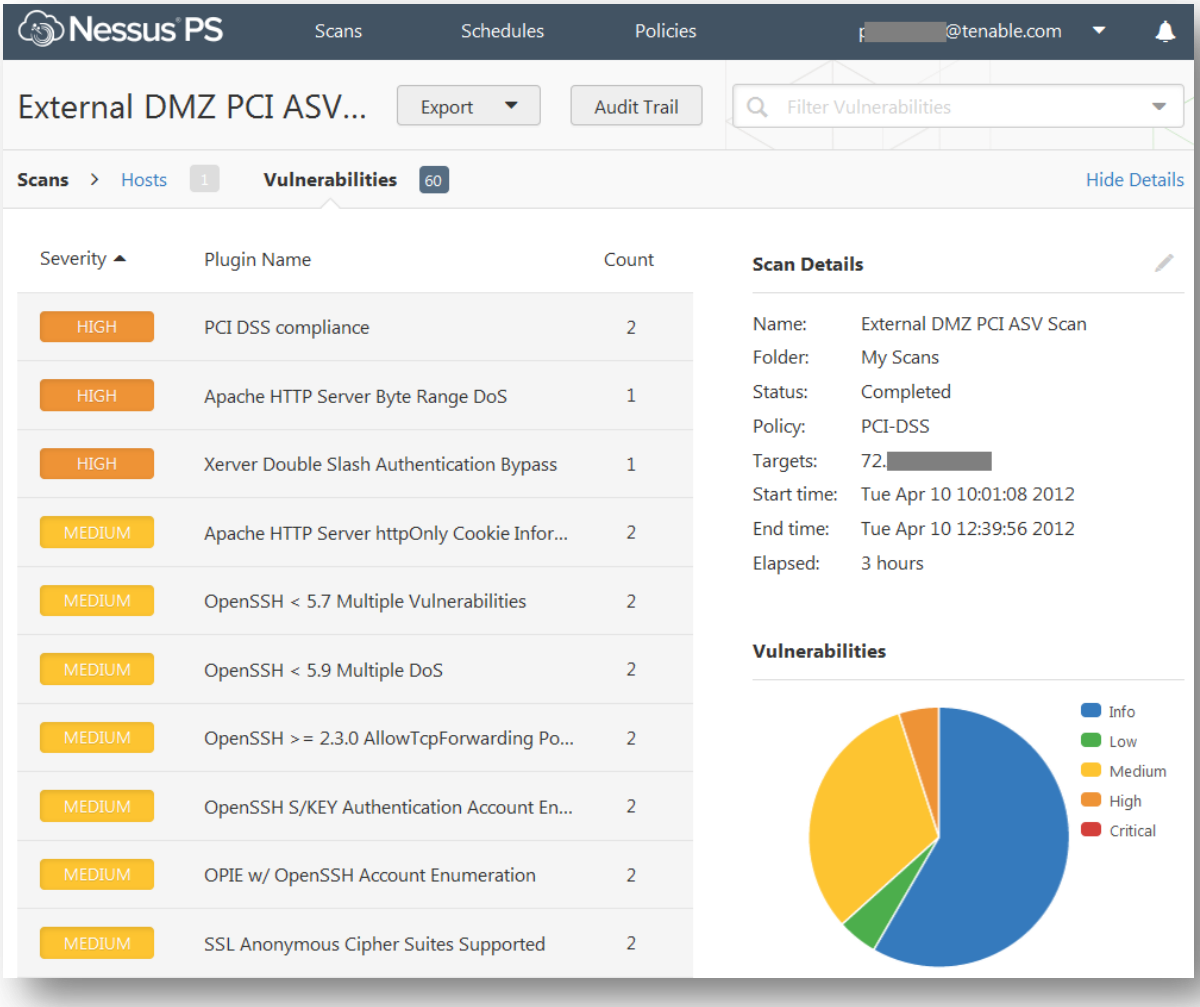


Revisión de los resultados de un análisis

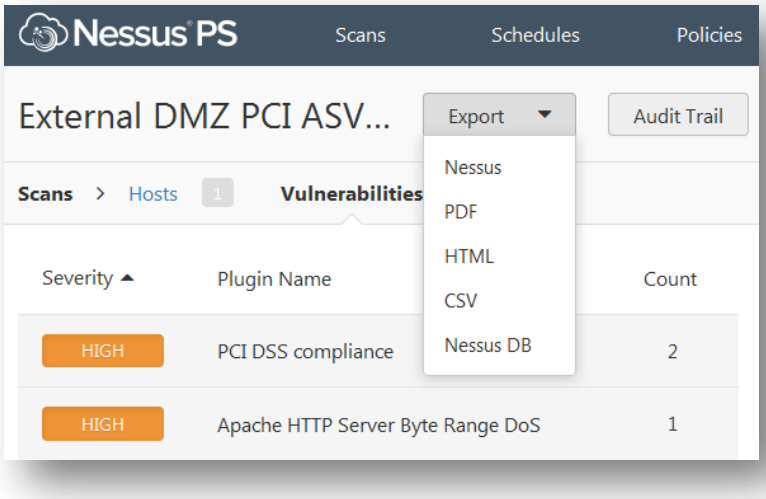
Una vez que finalizó un análisis, el estado aparecerá en la sección "**Scans**" (Análisis), junto con la fecha y hora en el que el análisis se actualizó por última vez o se finalizó.



El cliente tiene la opción de buscar el informe o descargarlo en varios formatos, como `.nessus`, CSV, PDF, HTML y formatos de archivo de Nessus DB.

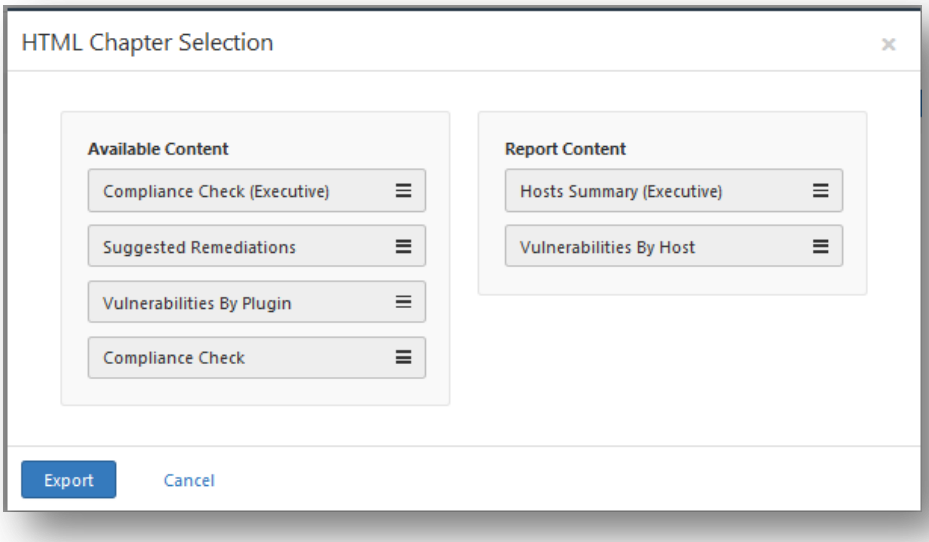


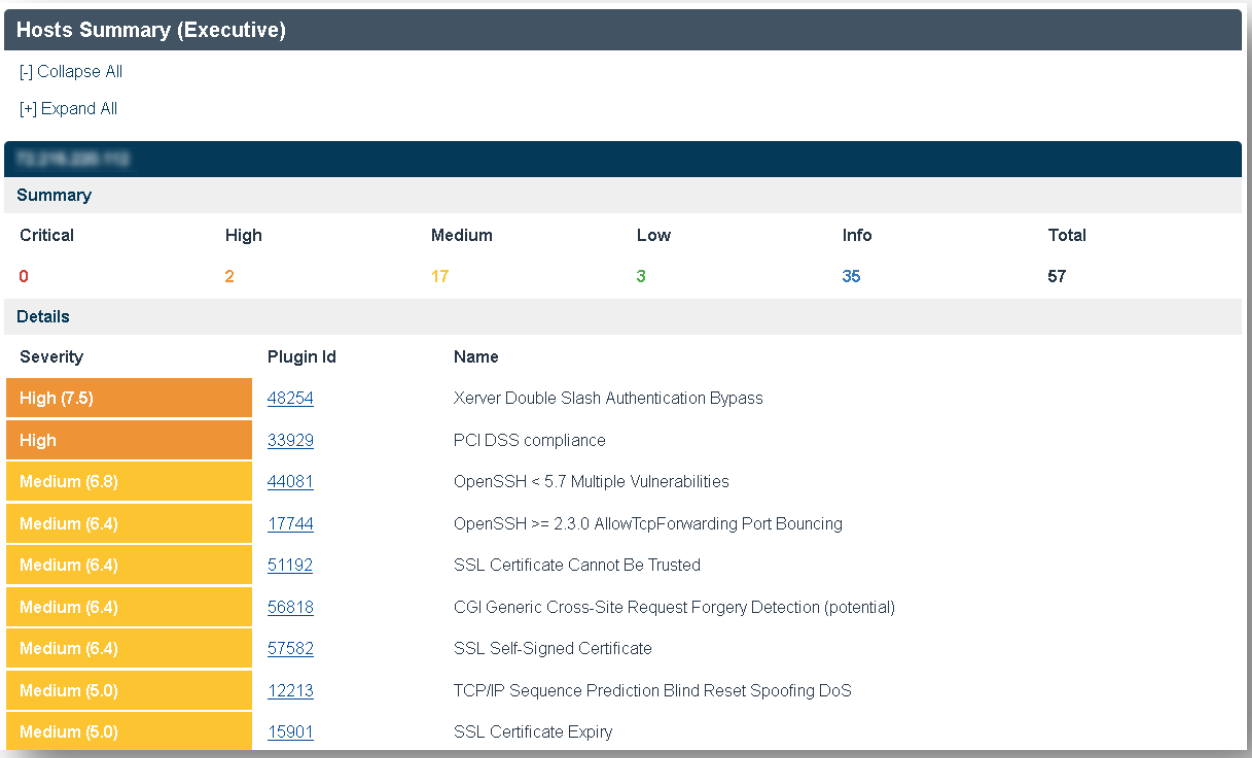
Análisis finalizado en la vista "Vulnerabilities" (Vulnerabilidades)



Opción Export (Exportación) para descargar el análisis actual

El formato HTML de descarga del informe posibilita en el mismo la selección de tipos de capítulo. Seleccione “HTML” como el formato de exportación y haga clic en los capítulos que quiere incluir en el resultado del informe:





Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

[redacted]

Summary

Critical	High	Medium	Low	Info	Total
0	2	17	3	35	57

Details

Severity	Plugin Id	Name
High (7.5)	48254	Xerver Double Slash Authentication Bypass
High	33929	PCI DSS compliance
Medium (6.8)	44081	OpenSSH < 5.7 Multiple Vulnerabilities
Medium (6.4)	17744	OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	56818	CGI Generic Cross-Site Request Forgery Detection (potential)
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12213	TCP/IP Sequence Prediction Blind Reset Spoofing DoS
Medium (5.0)	15901	SSL Certificate Expiry

Resultado del informe en formato HTML para Hosts Summary (Executive) (Resumen de hosts [Ejecutivo])

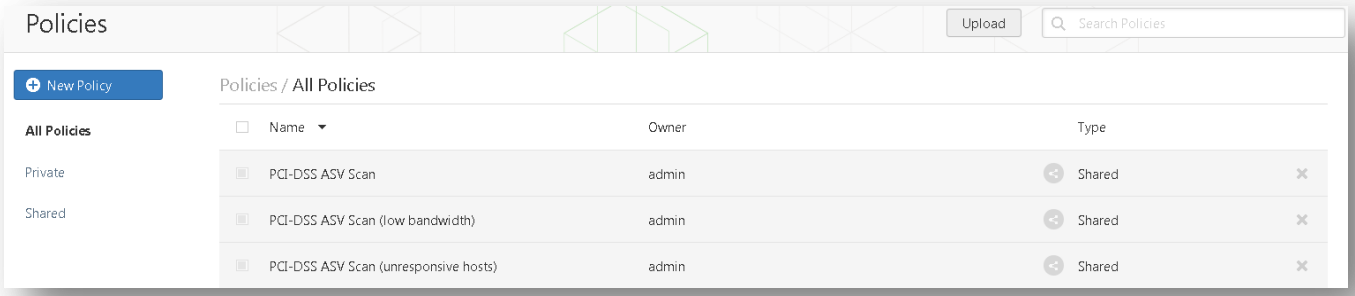
No existe un límite para la cantidad de análisis que pueden realizar e informes que pueden generar los clientes durante una suscripción activa al Nessus Perimeter Service. Puede encontrar información detallada sobre las directivas, los análisis y los informes de Nessus en la Guía del usuario de Nessus, aquí: http://www.tenable.com/products/nessus/documentation

Validación de ASV de PCI

Tenable Network Security, Inc. es un Proveedor de análisis aprobado (ASV) de PCI, y está certificado para validar análisis de vulnerabilidades de sistemas con conexión a Internet a fin de comprobar su observancia de determinados aspectos de los PCI Data Security Standards (PCI DSS) (Estándares de seguridad de datos de PCI). El Nessus Perimeter Service dispone de una directiva PCI DSS estática predefinida que cumple con los requisitos de análisis trimestral de PCI DSS v2.0. Los comerciantes y proveedores pueden utilizar esta directiva para evaluar inicialmente sus entornos según los requisitos de PCI DSS, y también ejecutar análisis de vulnerabilidades externasy generar informes que pueden ser validados por miembros calificados del personal de Tenable Network Security en lo que respecta al requisito de validación de ASV según PCI DSS. Vale aclarar que, si bien los clientes pueden utilizar la directiva de análisis PCI DSS para probar sus sistemas con conexión externa tan a menudo como lo deseen, deben enviar el análisis a Tenable para su validación a fin de que pueda considerárselo para calificar como análisis ASV de PCI válido. Los clientes tienen permitidos hasta dos envíos de informes trimestrales para la validación de ASV de PCI a través de Tenable Network Security, Inc.

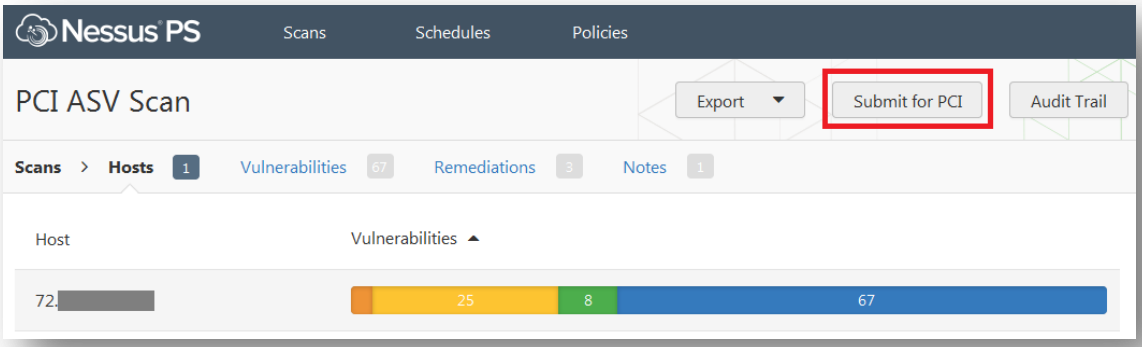
Una vez que iniciaron sesión en el servicio, los clientes tienen la opción de escoger una directiva llamada “PCI DSS”, que cumple con todos los requisitos de la PCI ASV Program Guide v2.0 (Guía del programa ASV de PCI v2.0), sección “ASV Scan Solution – Required Components” (Solución de análisis ASV – Componentes necesarios). Los clientes no tienen la capacidad de alterar ninguno de los parámetros preestablecidos de esta directiva.

Para calificar como análisis ASV según PCI DSS a fines de su validación a través del Nessus Perimeter Service, debe estar siempre seleccionada una de las tres directivas “PCI-DSS”.

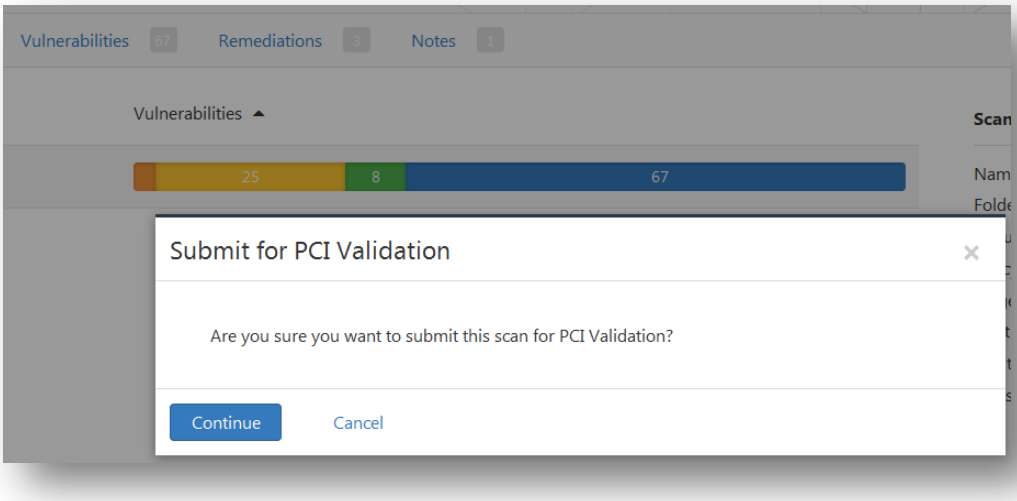


Envío de resultados de análisis para la revisión del cliente de PCI

Los clientes tienen la opción de enviar los resultados de sus análisis a Tenable Network Security para la validación de ASV de PCI. Si hace clic en “Submit for PCI” (Enviar para validación de PCI), los resultados del análisis se cargarán en una sección administrativa del Nessus Perimeter Service [el PCI Scanning Service (Servicio de análisis PCI)] para la revisión del cliente, y se le pedirá al cliente que inicie sesión en la sección de usuarios del servicio para examinar las conclusiones de los resultados del análisis desde una perspectiva de PCI DSS.



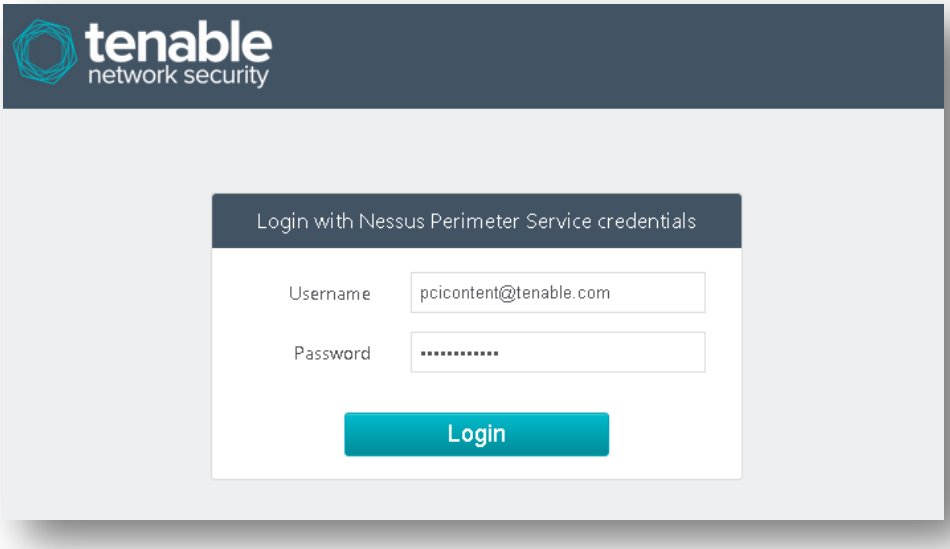
Enlace a “Submit for PCI” (Enviar para validación de PCI) (resaltado en rojo)



Cuadro de diálogo de carga de informe y enlace al PCI Scanning Service (Servicio de análisis PCI)

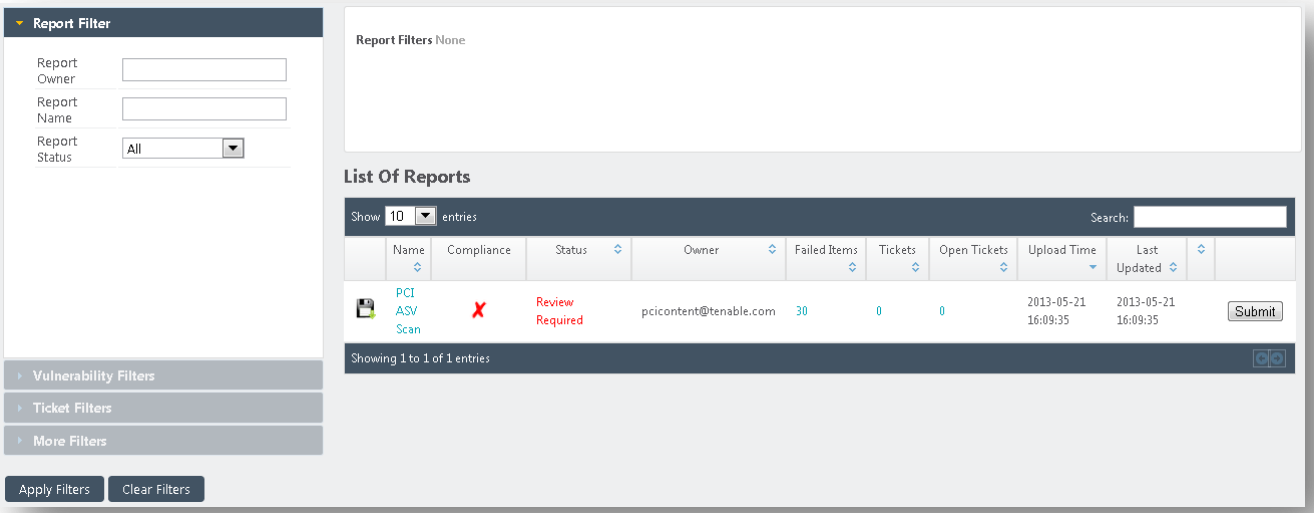
Se les pide encarecidamente a los clientes que revisen exhaustivamente los resultados de sus análisis PCI antes de enviar su(s) informe(s) a Tenable Network Security a través del PCI Scanning Service (Servicio de análisis PCI). Se requiere que los informes con resultados desaprobados atraviesen un ciclo de revisión completo del PCI Scanning Service (Servicio de análisis PCI); los clientes del Nessus Perimeter Service tienen un límite de dos (2) de estos ciclos por trimestre.

Interfaz de revisión del cliente



Pantalla de inicio de sesión del cliente en el PCI Scanning Service (Servicio de análisis PCI)

Una vez que el cliente inicia sesión en la PCI Validation user section (Sección de usuarios de validación PCI) aparece la lista de informes que fueron enviados a través de su acceso exclusivo del Nessus Perimeter Service. El “Report Filter” (Filtro de informes) permite filtrar los informes por Owner (propietario), Name (nombre) y Status (estado).



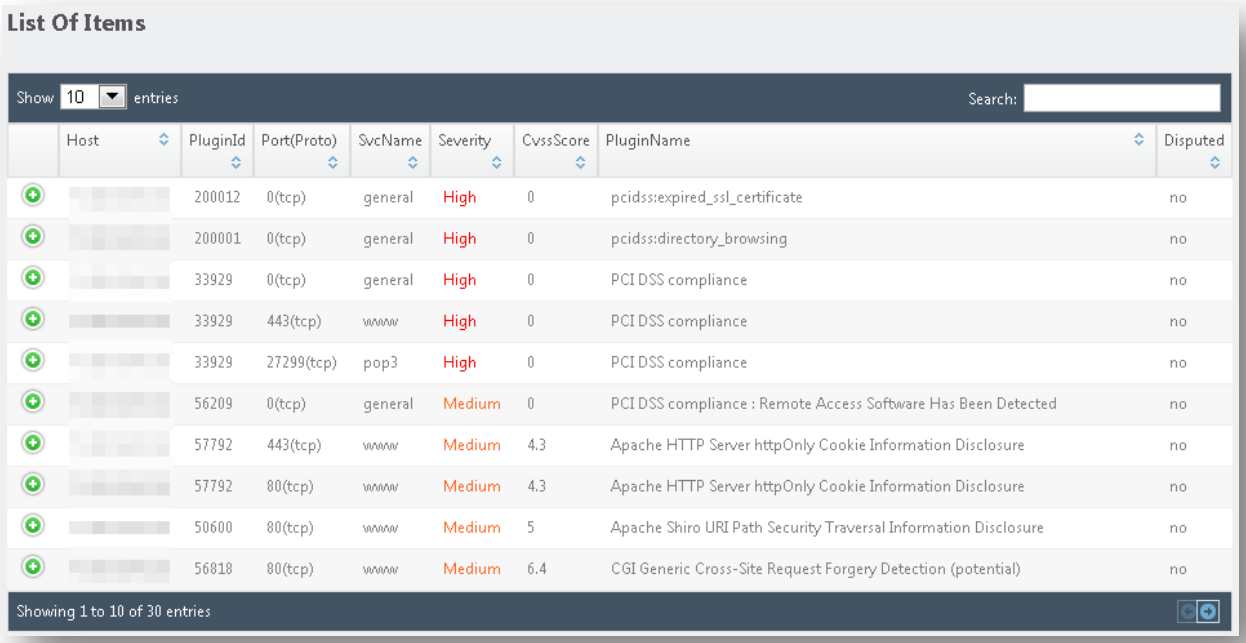
Revisión de los resultados de un análisis

Para aprobar una evaluación de ASV según PCI DSS, todos los elementos (a excepción de las vulnerabilidades de denegación de servicio o DoS) categorizados como “Critical” (Crítica), “High” (Alta) o “Medium” (Media) (o con una puntuación CVSS de 4.0 o más) deben estar corregidos o cuestionados por el cliente, y todos los elementos en conflicto (cuestionados) deben estar resueltos, aceptados como excepciones, aceptados como falsos positivos, o mitigados por medio de controles de compensación. Todos los elementos categorizados como “Crítical” (Crítica), “High” (Alta) o “Medium” (Media) en el Nessus Perimeter Service pueden verse en detalle, y todos los elementos tienen una opción para cuestionar.

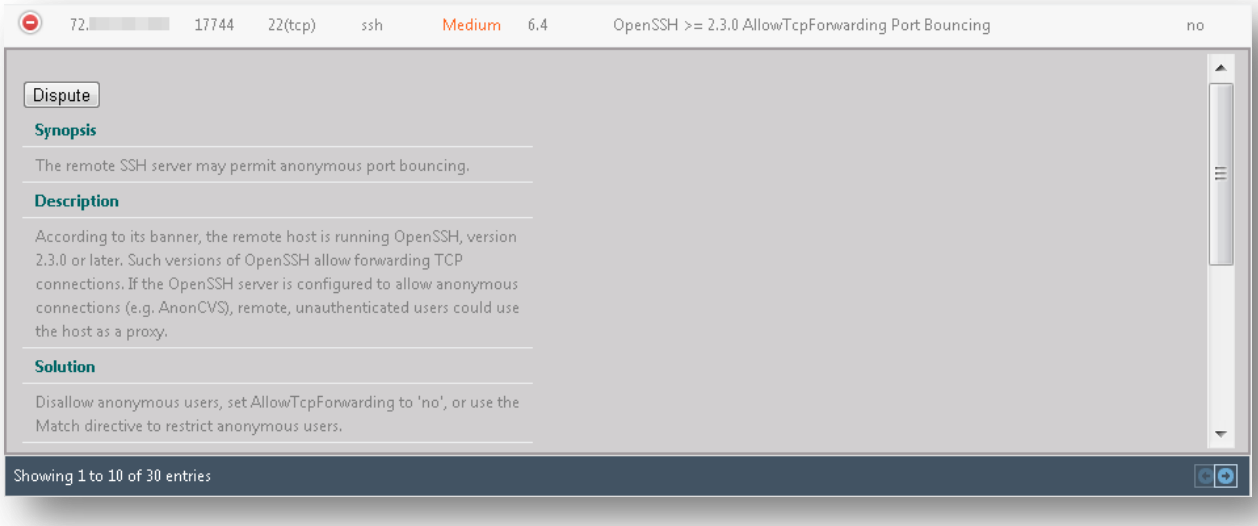
Si hace clic en el nombre del análisis en “List of Reports” (Lista de informes), el usuario puede ver una lista de hosts y la cantidad de vulnerabilidades encontradas en cada host, ordenadas por gravedad.

Si hace clic en la cantidad de “Failed Items” (Elementos con error) en “List of Reports” (Lista de informes), aparecerá una lista de elementos que deberán tratarse para que el informe ASV califique como “compatible” a través del PCI Scanning Service (Servicio de análisis PCI) de Tenable.

Los clientes del Nessus Perimeter Service/PCI Scanning Service (Servicio de análisis PCI) son responsables de revisar todos sus “Failed Items” (Elementos con error) antes de enviar un informe de análisis a Tenable Network Security. Si selecciona “Failed Items” (Elementos con error) en “List of Reports” (Lista de informes), podrá ir directamente a los elementos que pueden afectar el estado de compatibilidad de su validación de ASV de PCI.



Utilice el botón verde “+” de la primera columna de la izquierda para expandir una entrada individual y así ver más detalles de la vulnerabilidad.

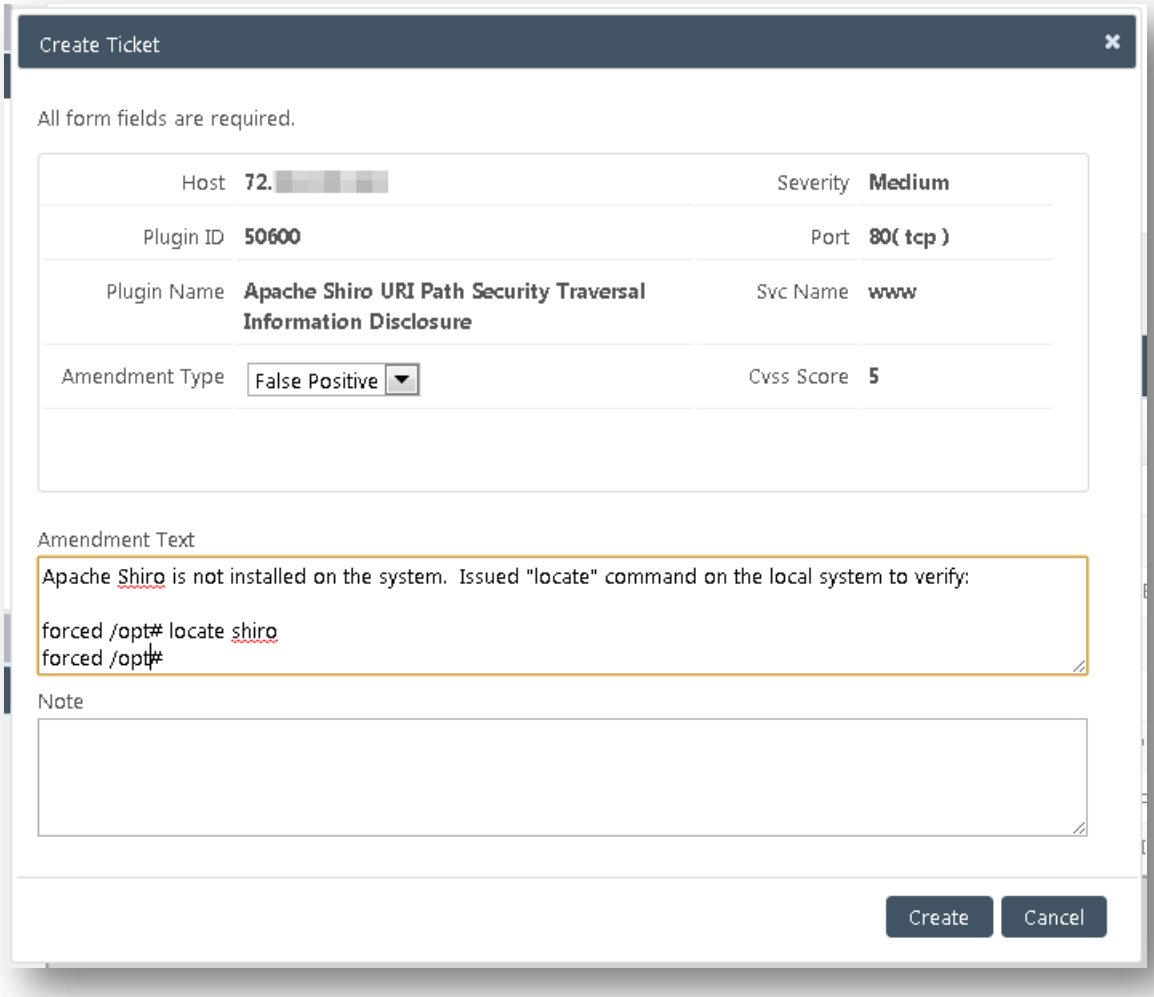


Descripción del elemento del informe de análisis con la funcionalidad “Dispute” (Cuestionamiento)

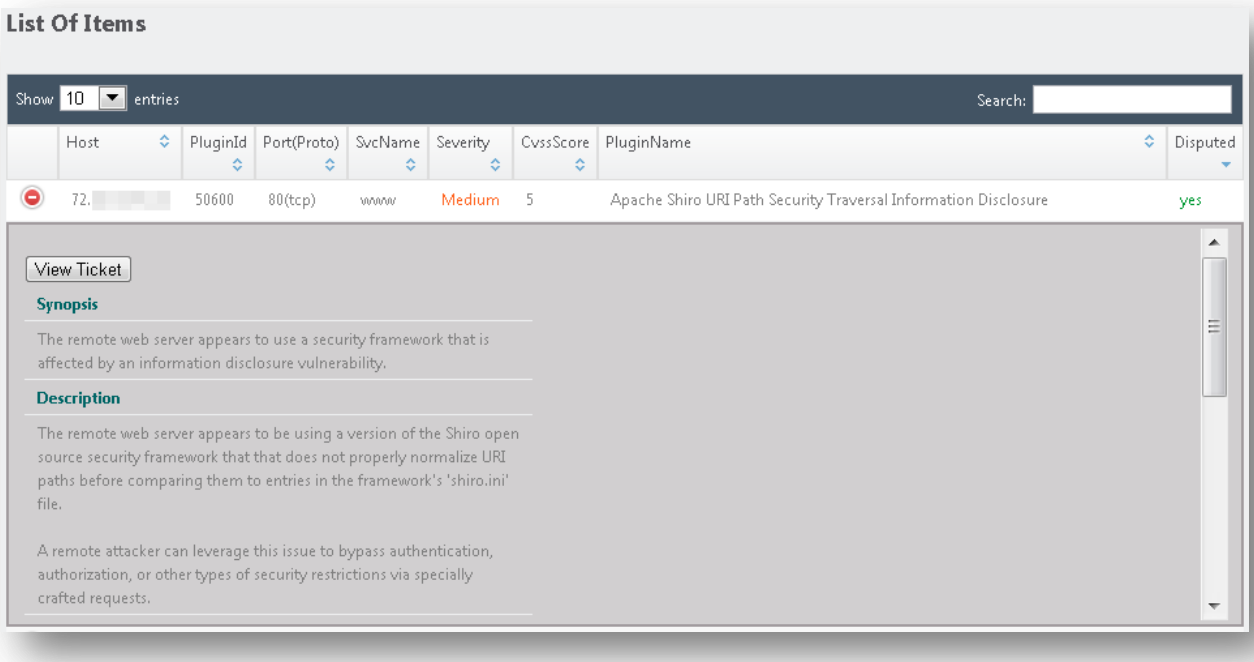
Como se muestra arriba, se visualiza un botón “Dispute” (Cuestionamiento) para cada elemento individual, lo que permite que el cliente introduzca más detalles acerca de la corrección de la vulnerabilidad o que cuestione lo que considera que puede ser un falso positivo generado por el análisis inicial.

Cuestionamiento de los resultados de un análisis

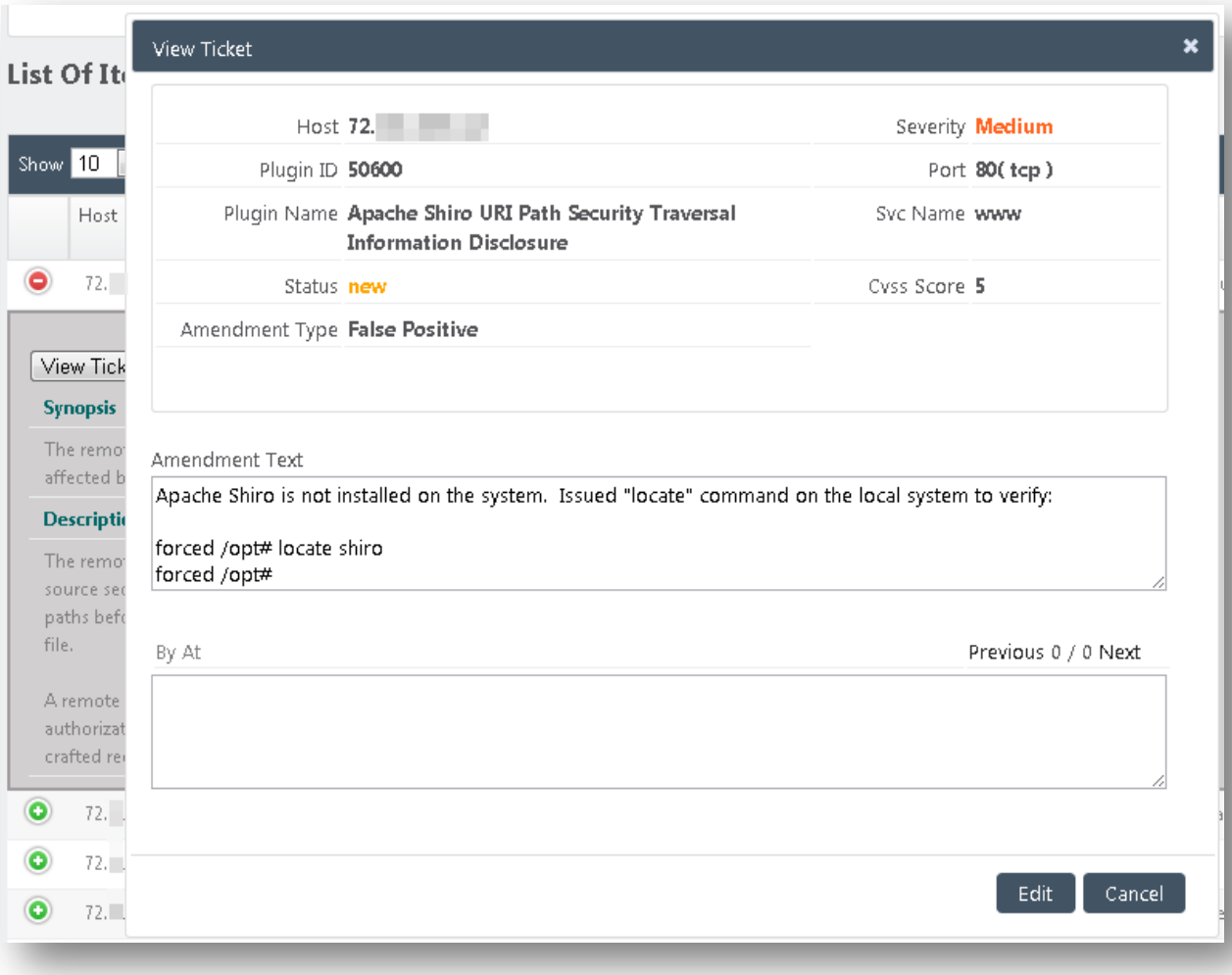
Cuando se cuestiona un elemento, se crea un ticket que permite la selección de un tipo de modificación, el agregado de texto a la modificación, y el agregado de cualquier otro comentario que el cliente quiera hacer antes de enviarlo para la revisión de Tenable Network Security.



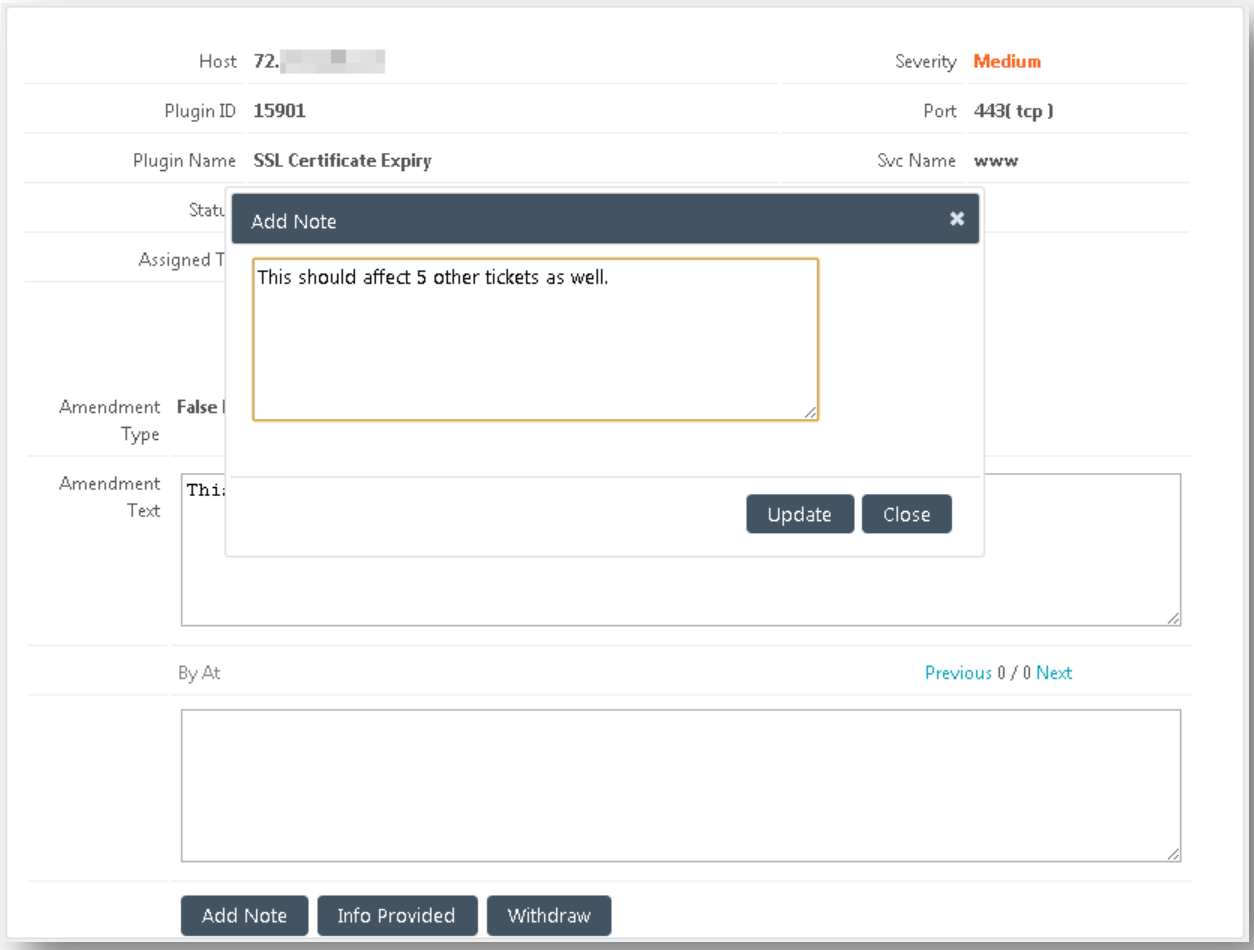
Una vez que se creó un ticket para un elemento específico, el cliente puede verlo seleccionando el elemento en cuestión y haciendo clic en “View Ticket” (Ver ticket).



Descripción del elemento del informe de análisis con la funcionalidad "View Ticket" (Ver ticket)



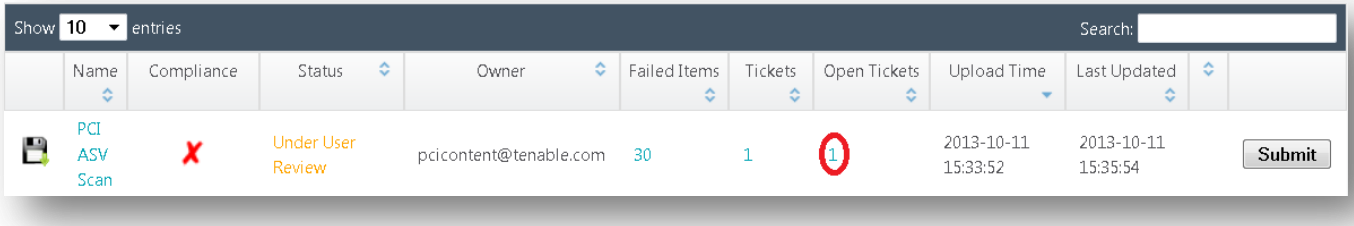
Puede agregar más comentarios haciendo clic en el botón “Edit” (Editar), luego en “Add Note” (Agregar nota), y guardar la nota en el ticket haciendo clic en “Update” (Actualizar).



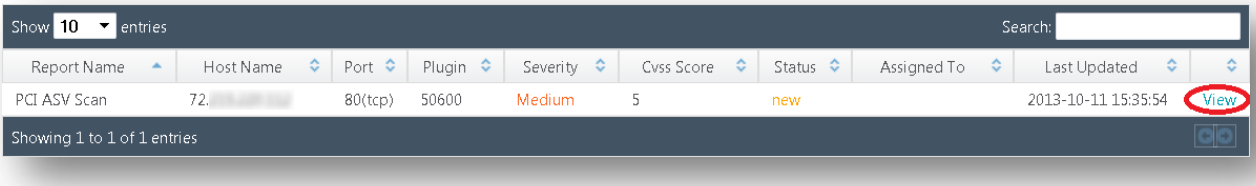
El plugin 33929, “PCI DSS Compliance”, es un plugin administrativo que vincula con los resultados de otros plugins. Si un informe muestra que un host no es compatible con PCI DSS, la resolución de todos los elementos con error permitirá que se resuelva el plugin 33929 y se reemplace por el plugin 33930, “PCI DSS Compliance: Passed (Compatibilidad PCI DSS: aprobada). En casos de cuestionamientos o excepciones, si se cuestionan o se exceptúan correctamente todos los elementos con error en el informe, se puede dar una excepción para el plugin 33929 en base a la solución del resto de los problemas del informe.

Envío de adjuntos como evidencia para un cuestionamiento

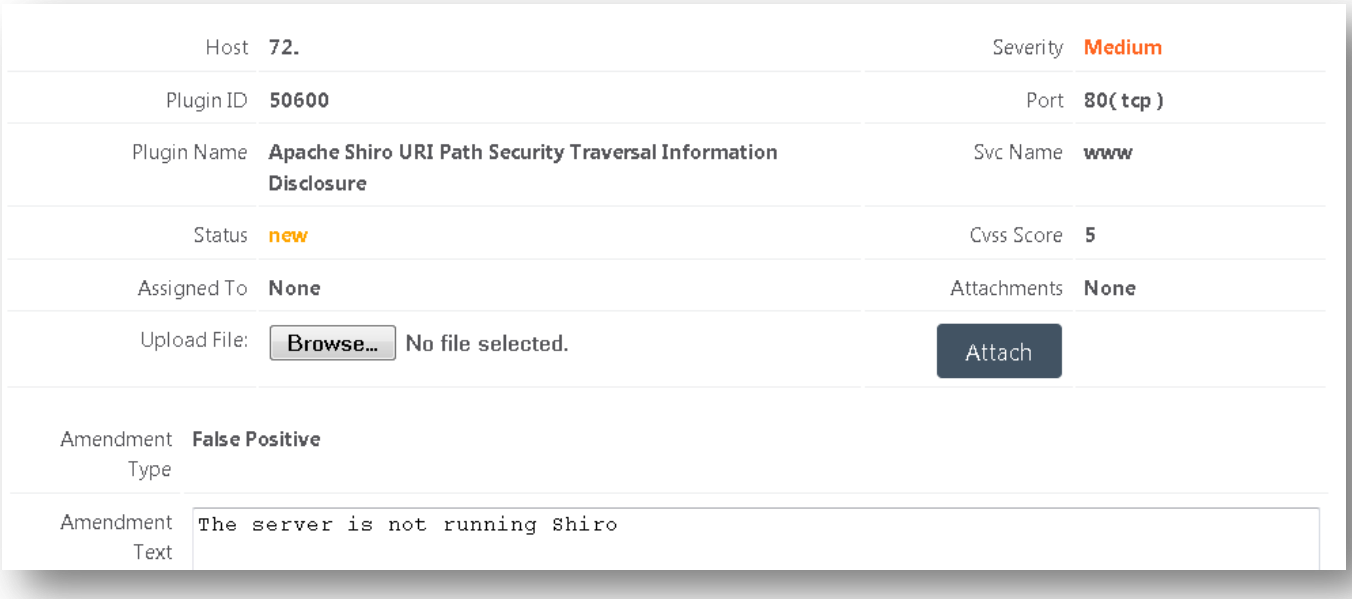
Una vez que se creó un ticket, es posible enviar evidencia de respaldo como adjunto. Después de crear un ticket, haga clic en el número que está debajo de “Open Tickets” (Tickets abiertos) para ver todos los tickets abiertos:



En la pantalla “List of Tickets” (Lista de tickets), haga clic en “View” (Ver):



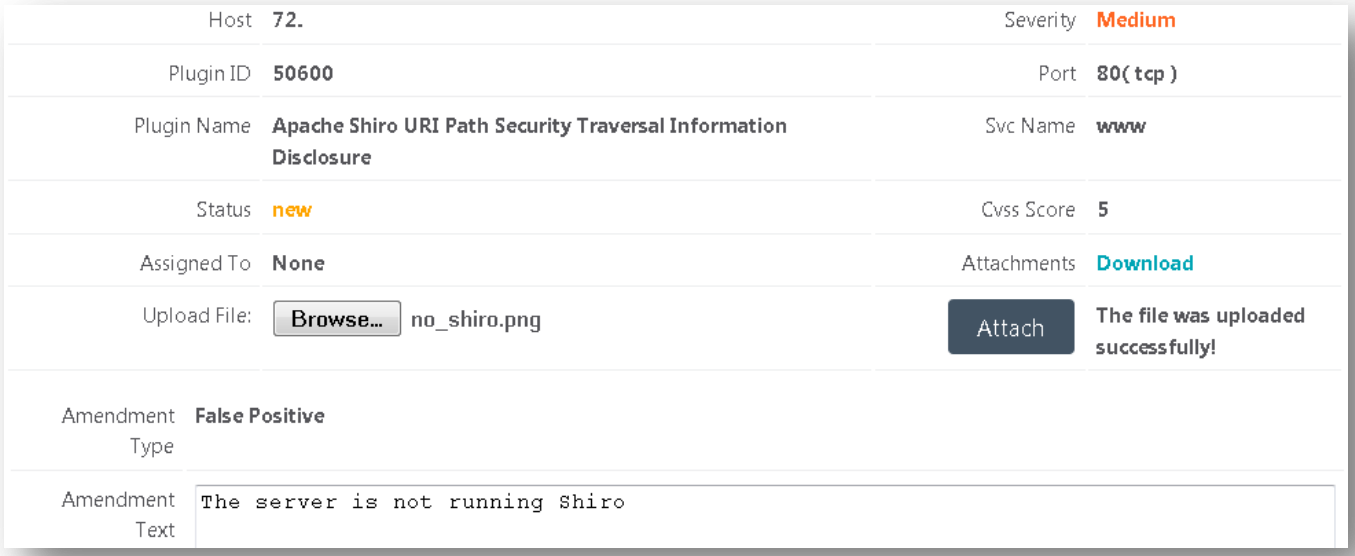
Cuando vea la pantalla del ticket abierto, puede ver las opciones “Upload File” (Cargar archivo) y “Attach” (Adjuntar):



Haga clic en “Browse…” (Explorar...) para buscar el archivo de evidencia (captura de pantalla, documento de Word, PDF, etc.) que quiere cargar:

Archivo de evidencia de muestra (no_shiro.png)

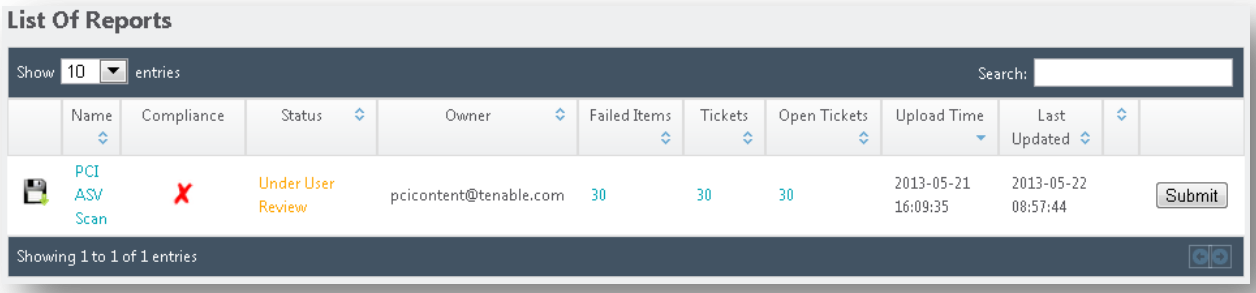
Luego, haga clic en “Attach” (Adjuntar) para adjuntar el archivo al ticket. Una vez finalizado, la pantalla mostrará un mensaje que dice que el archivo se cargó correctamente:



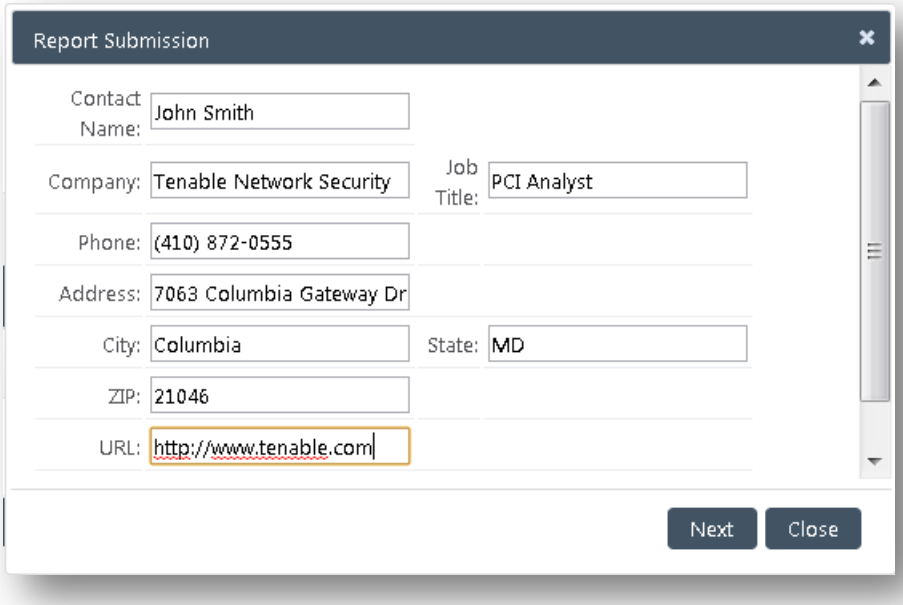
Si hace clic en el enlace “Download” (Descargar) junto a “Attachments” (Adjuntos), verá los nombres de todos los archivos adjuntos en el ticket.

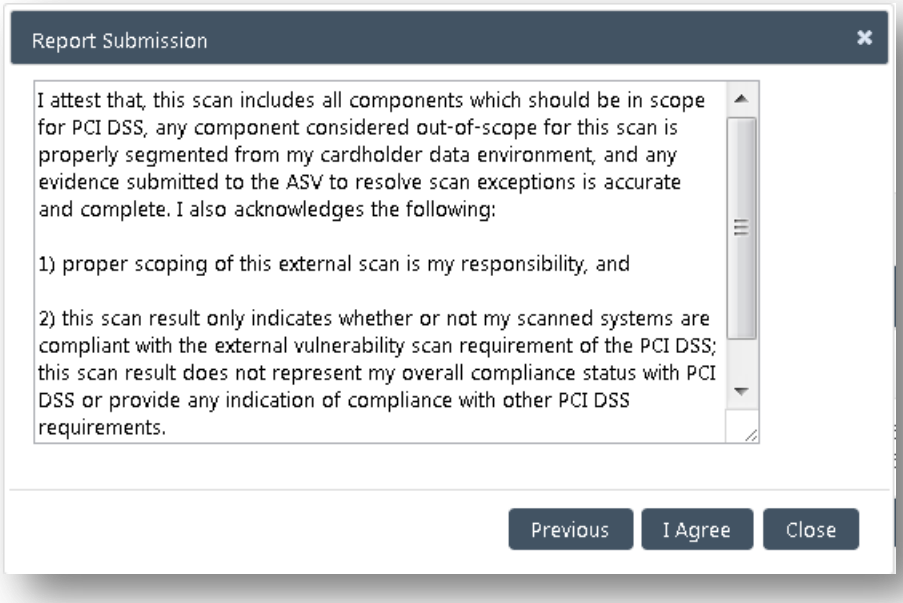
Envío de un informe de análisis para la revisión de Tenable

Cuando se hayan creado tickets para todos los elementos del informe pendientes bajo revisión del usuario, puede enviar el informe a Tenable Network Security para la revisión de ASV.



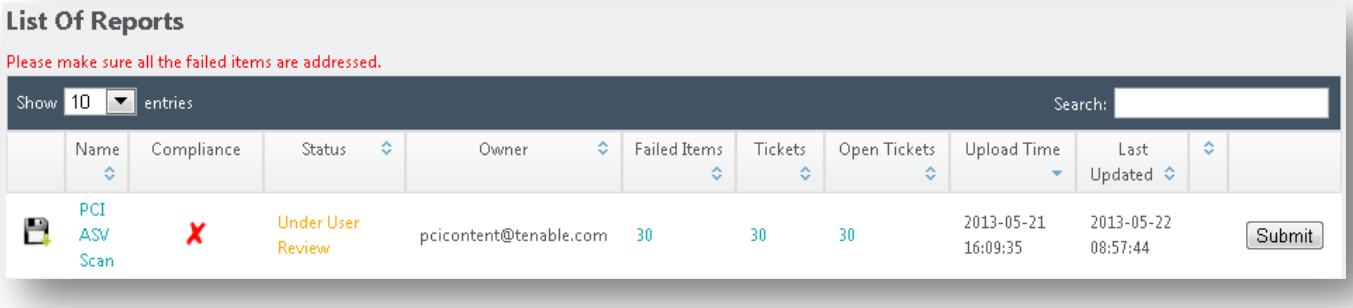
Antes de poder enviar un informe para su revisión, el cliente debe completar su información de contacto y aceptar una atestación que incluye texto obligatorio, según se describe en la ASV Program Guide (Guía del programa de ASV).



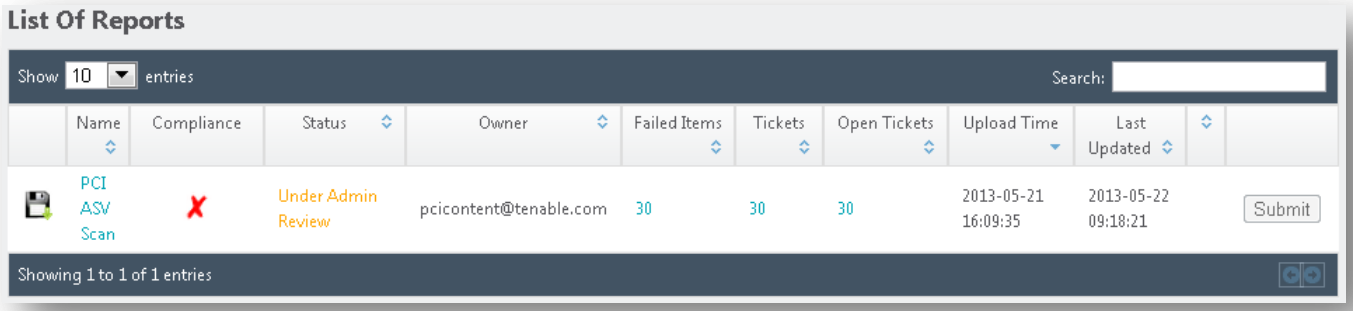


Texto de atestación de envío de informe

Si un cliente no trata algún elemento pendiente en un análisis específico antes de enviar el informe para su revisión de ASV, se le indicará que se asegure de que se haya creado un ticket para cada elemento. No se puede enviar a Tenable Network Security para su revisión ningún informe con elementos pendientes que no hayan sido tratados por el cliente.



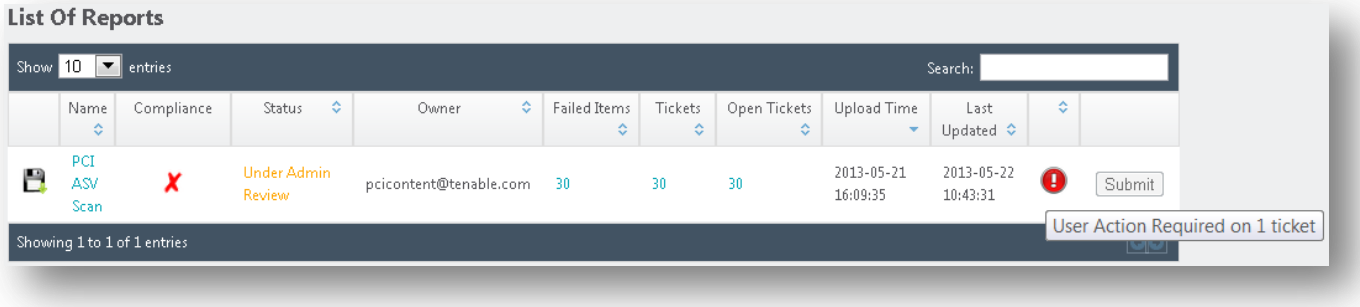
Cuando finalmente se envía un informe a Tenable Network Security para su revisión, el estado del informe cambia de "Under User Review" (En revisión del usuario) a "Under Admin Review" (En revisión del administrador), y la opción "Submit" (Enviar) desaparece (se ve en gris) para evitar que se envíen elementos o informes duplicados.



Informe enviado con estado "Under Admin Review" (En revisión del administrador)

La función "Withdraw" (Retirar) en un ticket abierto sólo está disponible una vez que el informe se haya enviado para la revisión a través del PCI Scanning Service (Servicio de análisis PCI) de Tenable. Tenga cuidado al usar la función "Withdraw" (Retirar); si retira un ticket, el elemento en cuestión se marcará como sin resolución por contener pruebas no concluyentes, y el informe completo será considerado como no compatible.

Si un miembro del personal de Tenable Network Security le solicita más información, o si es necesaria cualquier otra acción de usuario por parte del cliente para un ticket, aparecerá un indicador en la "List of Reports" (Lista de informes) del cliente, como se muestra a continuación:

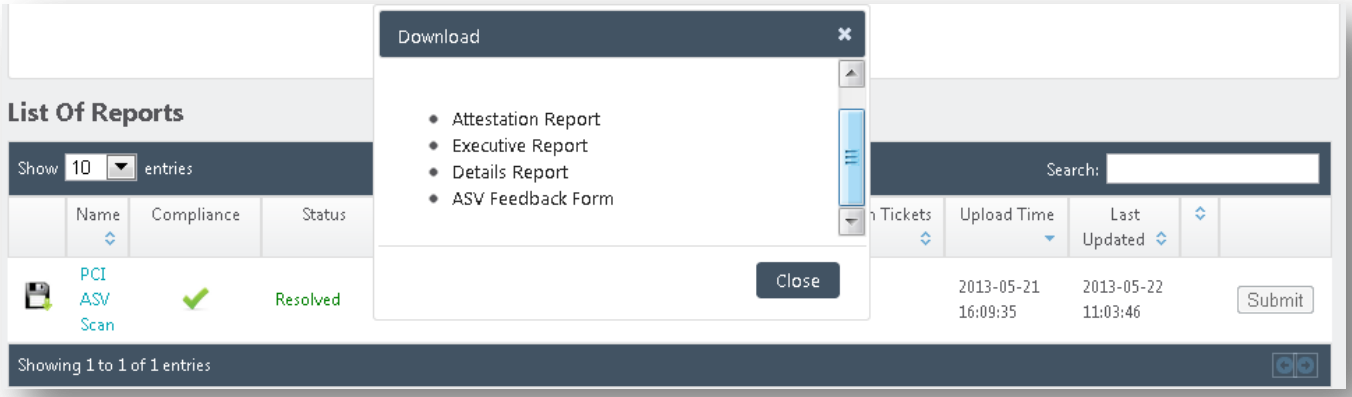


Notificación "User Action Required" (Se requiere acción del usuario)

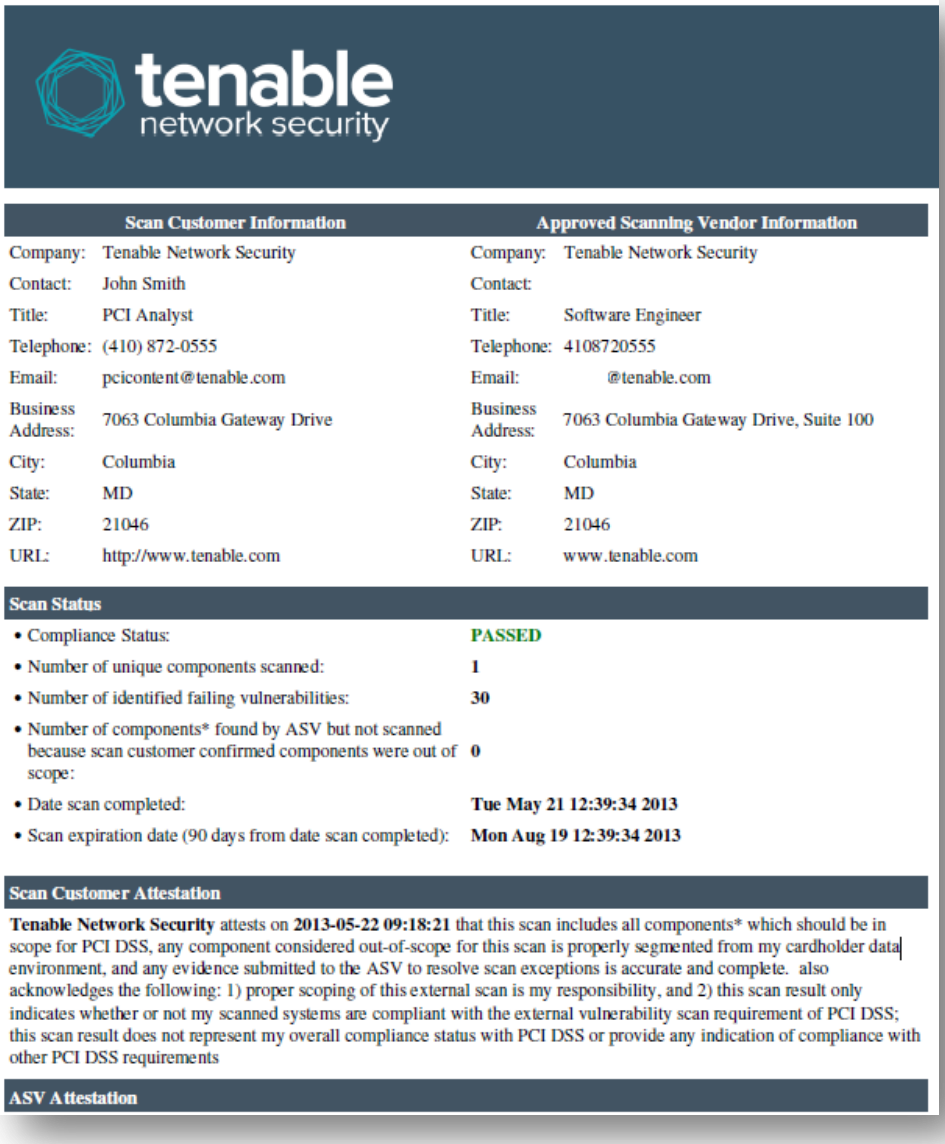
Luego, el usuario puede modificar el ticket y volver a enviarlo a Tenable Network Security para una nueva revisión.

Formatos de informe ASV de PCI

Una vez que un informe de análisis recibió el estado “compliance” (compatibilidad) del PCI Scanning Service (Servicio de análisis PCI) de Tenable, los clientes tienen la opción de ver los informes en los formatos “Attestation Report” (Informe de atestación), “Executive Report” (Informe ejecutivo) o “Details Report” (Informe detallado). El cliente del Nessus Perimeter Service recibe también un ASV Feedback Form (Formulario de comentarios de ASV). Estas opciones están disponibles por medio del ícono “Download” (Descargar), junto a cada informe.



Los informes Attestation Report (Informe de atestación), Executive Report (Informe ejecutivo) y Details Report (Informe detallado) solo están disponibles para el cliente en formato PDF, y no pueden modificarse.



tenable network security

Scan Customer Information		Approved Scanning Vendor Information	
Company:	Tenable Network Security	Company:	Tenable Network Security
Contact:	John Smith	Contact:	
Title:	PCI Analyst	Title:	Software Engineer
Telephone:	(410) 872-0555	Telephone:	4108720555
Email:	pcicontent@tenable.com	Email:	@tenable.com
Business Address:	7063 Columbia Gateway Drive	Business Address:	7063 Columbia Gateway Drive, Suite 100
City:	Columbia	City:	Columbia
State:	MD	State:	MD
ZIP:	21046	ZIP:	21046
URL:	http://www.tenable.com	URL:	www.tenable.com

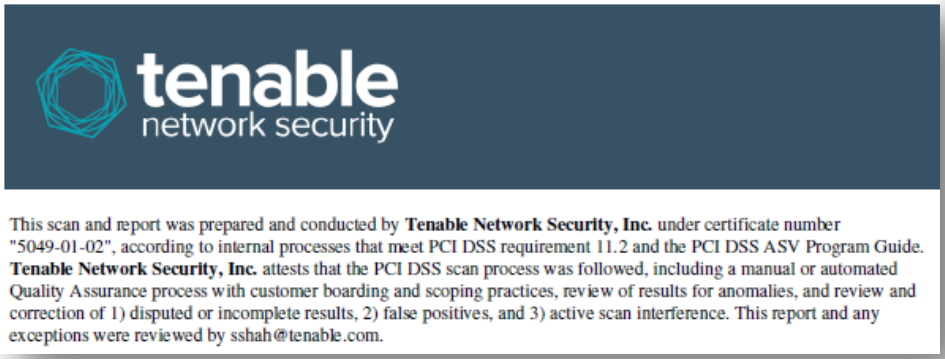
Scan Status

- Compliance Status: **PASSED**
- Number of unique components scanned: **1**
- Number of identified failing vulnerabilities: **30**
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- Date scan completed: **Tue May 21 12:39:34 2013**
- Scan expiration date (90 days from date scan completed): **Mon Aug 19 12:39:34 2013**

Scan Customer Attestation

Tenable Network Security attests on **2013-05-22 09:18:21** that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements

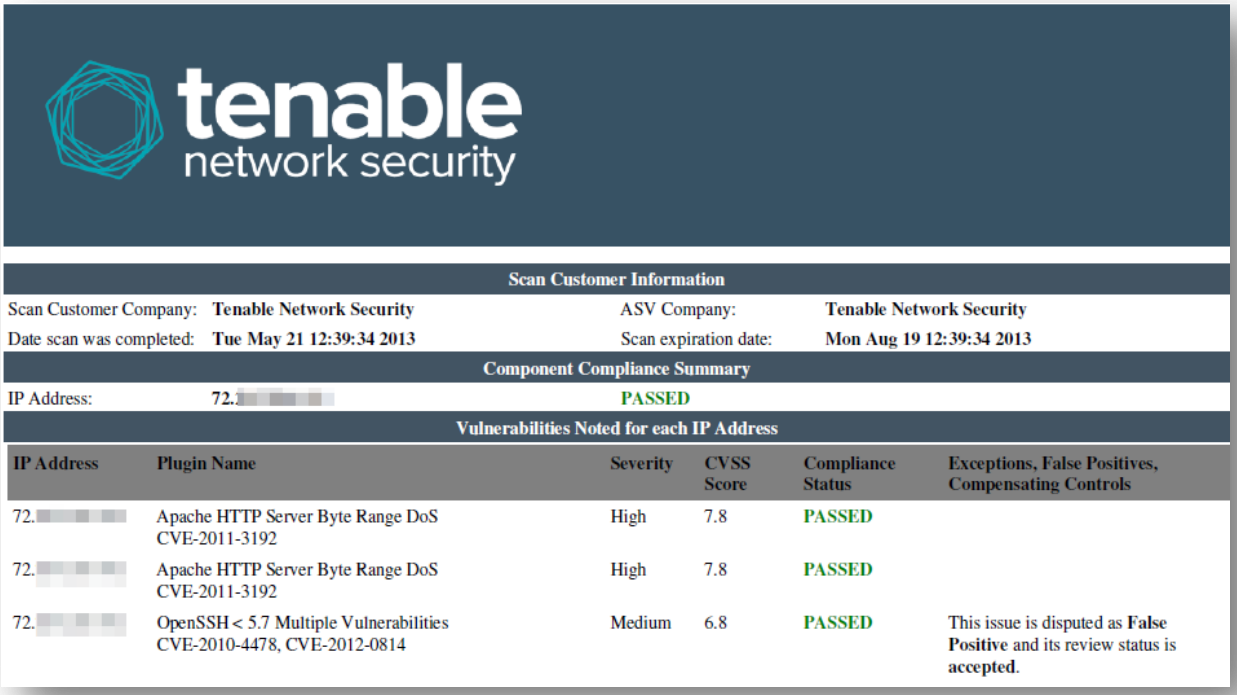
ASV Attestation



tenable network security

This scan and report was prepared and conducted by **Tenable Network Security, Inc.** under certificate number "5049-01-02", according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. **Tenable Network Security, Inc.** attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by sshah@tenable.com.

Muestra de Attestation Report (Informe de atestación)



tenable network security

Scan Customer Information			
Scan Customer Company:	**Tenable Network Security**	ASV Company:	**Tenable Network Security**
Date scan was completed:	**Tue May 21 12:39:34 2013**	Scan expiration date:	**Mon Aug 19 12:39:34 2013**

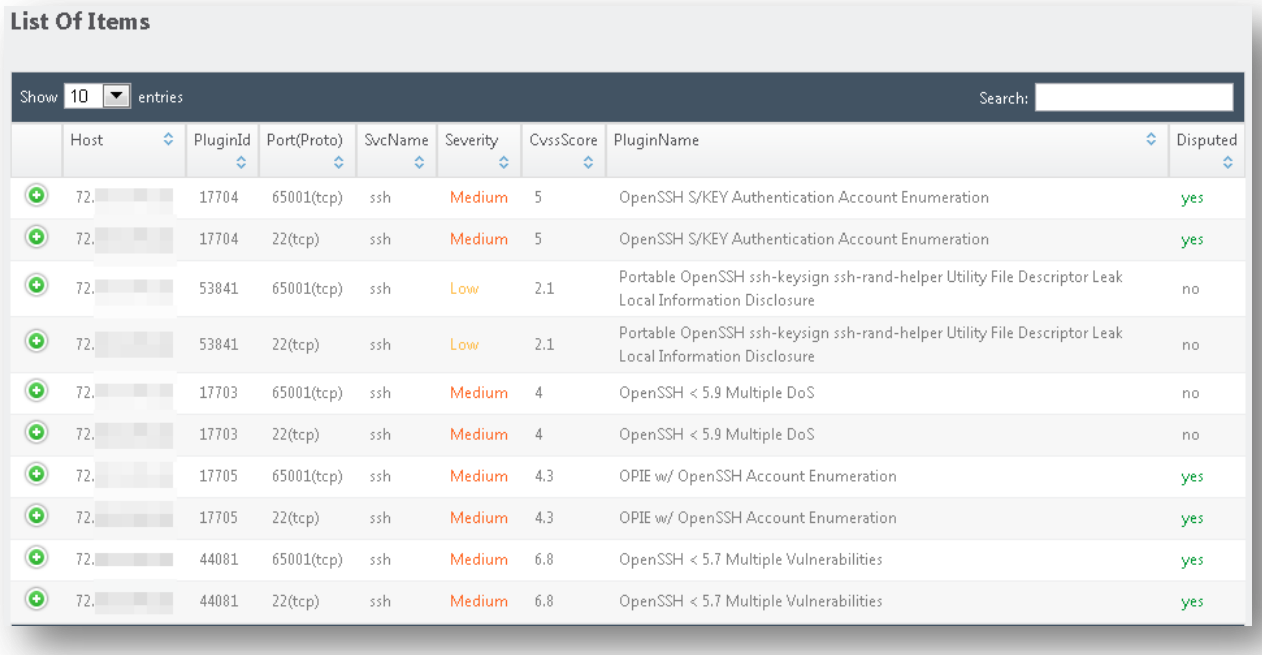
Component Compliance Summary		
IP Address:	72.	**PASSED**

Vulnerabilities Noted for each IP Address

IP Address	Plugin Name	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, Compensating Controls
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	**PASSED**	
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	**PASSED**	
72.	OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814	Medium	6.8	**PASSED**	This issue is disputed as **False Positive** and its review status is **accepted**.

Muestra de Executive Report (Informe ejecutivo)

Cuando se selecciona un nombre de informe y de host en la interfaz web, se muestra una lista de elementos relacionados con el informe seleccionado.



List Of Items

Show 10 entries Search:

Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
72.	17704	65001(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
72.	17704	22(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
72.	53841	65001(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
72.	53841	22(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
72.	17703	65001(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
72.	17703	22(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
72.	17705	65001(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
72.	17705	22(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
72.	44081	65001(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes
72.	44081	22(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes

"List of Items" (Lista de elementos) visualizada en la interfaz web

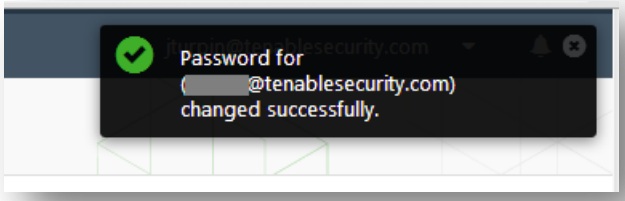
Soporte

Cuando compra una suscripción al Nessus Perimeter Service de Tenable, Tenable recibe el nombre y la dirección de correo electrónico de la(s) persona(s) de contacto técnico. Se crea automáticamente una cuenta independiente en el Tenable Support Portal (Portal de soporte de Tenable) para cada persona de contacto técnico. Las solicitudes de soporte son aceptadas a través del Portal, pero también puede enviar un correo electrónico a support@tenable.com. Tenga en cuenta que las solicitudes por correo electrónico **deben** enviarse desde una de las direcciones de correo electrónico proporcionadas a Tenable como contacto de soporte.

Cambio de la contraseña

Si necesita cambiar la contraseña del Nessus Perimeter Service, haga clic en su dirección de correo electrónico en la esquina superior derecha de la pantalla del analizador y escoja la opción “User Profile” (Perfil de usuario) en la lista desplegable.

Después de cambiar su contraseña, aparecerá un cuadro de diálogo que lo confirme:



Para obtener más información

Puede obtener la documentación de Nessus aquí:

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

Puede encontrar más información acerca de las características del Tenable Support Portal (Portal de soporte de Tenable) aquí:

http://www.tenable.com/whitepapers/tenable-network-security-support-portal

http://static.tenable.com/prod_docs/Subscription_Agreement.pdf

Si tiene algún problema con el proceso de inscripción, contáctese con licenses@tenable.com.

El Nessus Perimeter Service solo brinda soporte por correo electrónico. Envíe todas las preguntas de soporte a support@tenable.com e incluya su Customer ID (Identificación de cliente) con una descripción detallada del problema que experimenta. También puede acceder al Tenable Support Portal (Portal de soporte de Tenable) para generar un ticket de soporte.

Acerca de Tenable Network Security

Más de 20000 organizaciones confían en Tenable Network Security, entre ellas el Departamento de Defensa de EE. UU. en su totalidad y muchas de las compañías más grandes y los gobiernos de todo el mundo, para adelantarse a las vulnerabilidades, amenazas y riesgos de compatibilidad emergentes. Sus soluciones Nessus y SecurityCenter siguen marcando la norma para identificar vulnerabilidades, evitar ataques y cumplir con muchísimos requisitos regulatorios. Para obtener más información, visite www.tenable.com.

SEDE CENTRAL MUNDIAL

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