# Guía del usuario de Nessus Perimeter Service

**24 de octubre de 2012**

***(Revisión 4)***

# Índice

# Introducción

En este documento se describe el Nessus Perimeter Service (Servicio de perímetro de Nessus) 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, y el soporte del Perimeter Service.

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.

Este documento ha sido traducido de una versión originalmente redactada en inglés. Parte del texto aparece en inglés para mostrar cómo está representado en el producto.

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 la red 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 compatibilidd 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’s Online Store (Tienda en línea de Tenable). Para obtener información sobre los precios, visite la Tienda en línea de Tenable o envíe su consulta a subscriptions@tenable.com.

Un paquete de suscripción al Nessus Perimeter Service comprende:

- Análisis ilimitado de los IP 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 PCI ASV a través de Tenable Network Security, Inc.
- Acceso en todo momento al 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 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:


*Pantalla de inicio de sesión del Nessus Perimeter Service*

## 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 su red con conexión externa. Esta directiva contiene la configuración predeterminada que ejecutará un análisis de perímetro exhaustivo:
  - Un análisis rápido de puertos de 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 rápido de puertos 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 la o 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 la aplicación, 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 con PCI DSS. Puede encontrar más información acerca de la ejecución de análisis con la directiva ASV de PCI DSS  ASV y la validación de análisis a través del servicio PCI ASV 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.

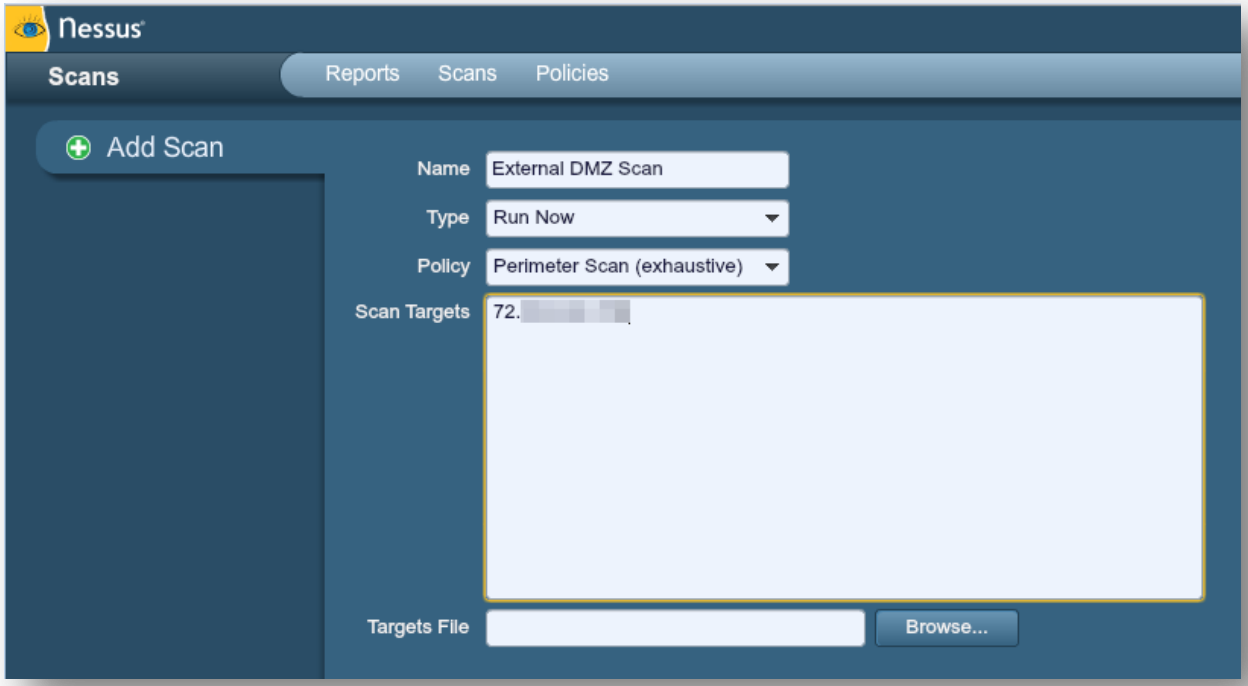

El personal de Tenable revisa y actualiza periódicamente estas directivas para garantizar que incluyan actualizaciones para familias de plugins y otras mejoras a la configuración. Los clientes no tienen la capacidad de ver ni alterar ninguno de los parámetros preestablecidos de la directiva PCI DSS.

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.

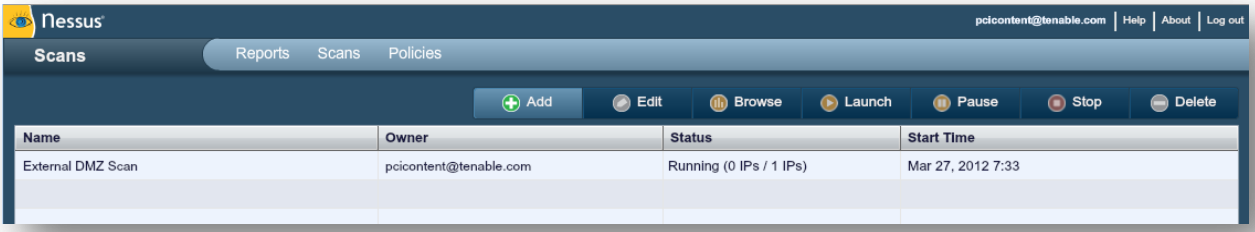
El botón “**Import Policy**” **(Importar directiva)** situado en la esquina superior izquierda le permitirá cargar en el analizador del Perimeter Service las directivas creadas con anterioridad. Mediante el cuadro de diálogo “**Browse…**” **(Explorar)**, seleccione la directiva de su sistema local y 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 “Add” (Agregar). Luego introduce un nombre exclusivo para el 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. También puede editar análisis ya agregados como plantillas para cambiar el nombre del análisis, el o los destinos del análisis y la directiva de análisis.



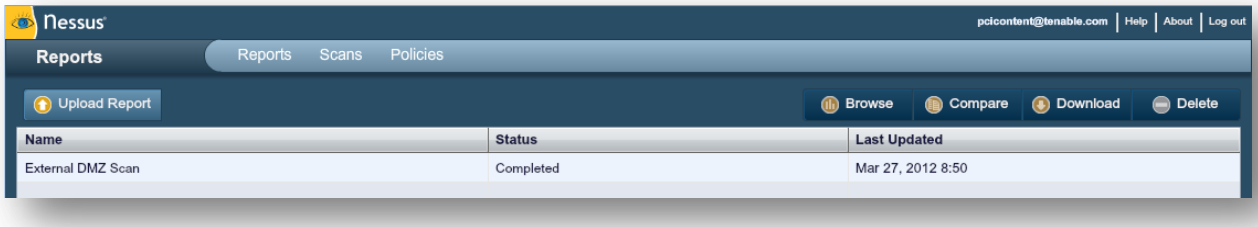

Para iniciar un análisis el cliente selecciona la sección “Scans” (Análisis), resalta el análisis configurado deseado, y selecciona “Launch” (Iniciar).




Una vez que comenzaron, los análisis pueden ponerse en pausa o detenerse durante el proceso seleccionando los botones “Pause” (Pausar) o “Stop” (Detener) en la página “Scans” (Análisis) del Nessus Perimeter Service. Los resultados obtenidos de un análisis actualmente en curso pueden verse resaltando ese análisis en particular y seleccionando el botón “Browse” (Explorar).

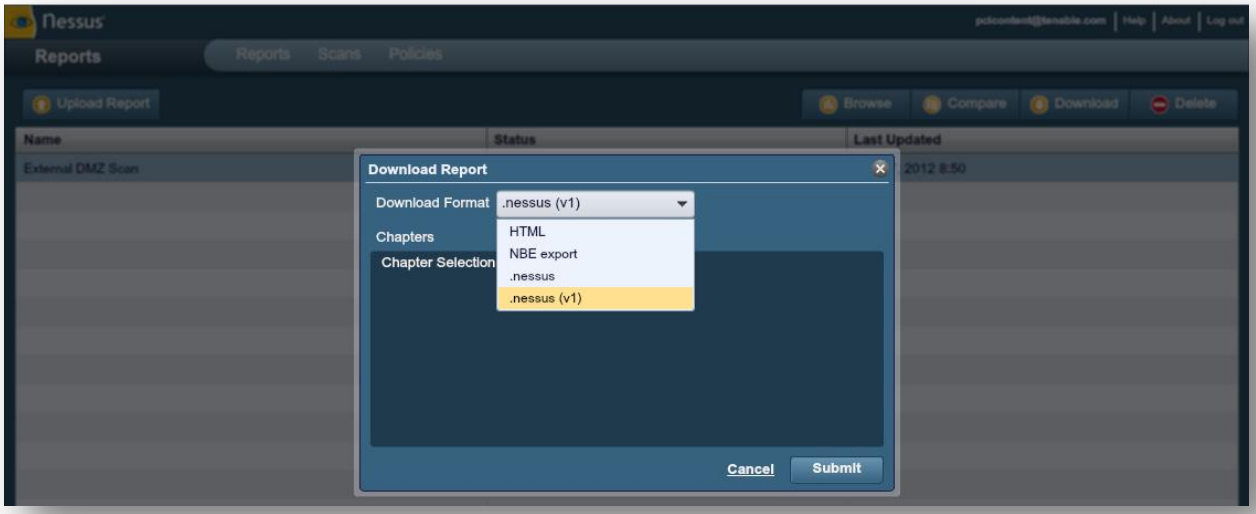
## Revisión de los resultados de un análisis

Una vez que finalizó un análisis, el estado aparecerá en la sección “Reports” (Informes), junto con el horario en el que el análisis se actualizó por última vez o se finalizó.



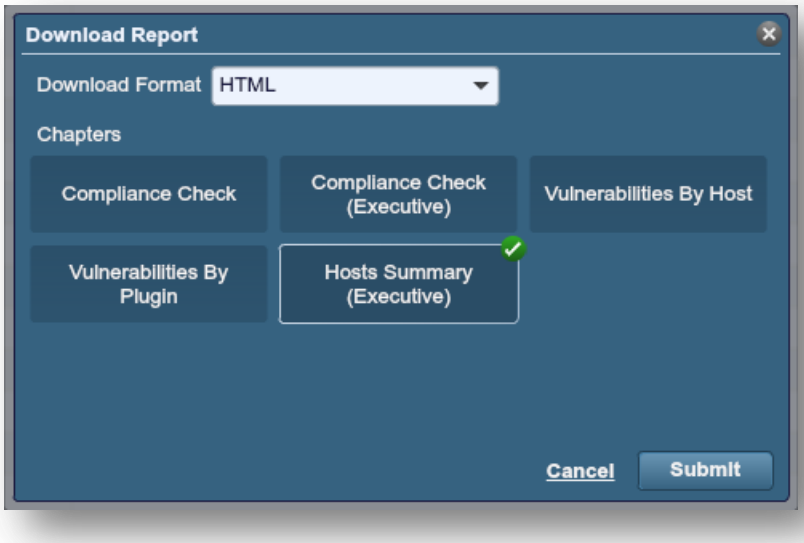

El cliente tiene la opción de ver el análisis o descargar el informe en varios formatos, como **`.nessus`**, **`.nessus`** (v1), NBE export y formatos de archivo HTML.

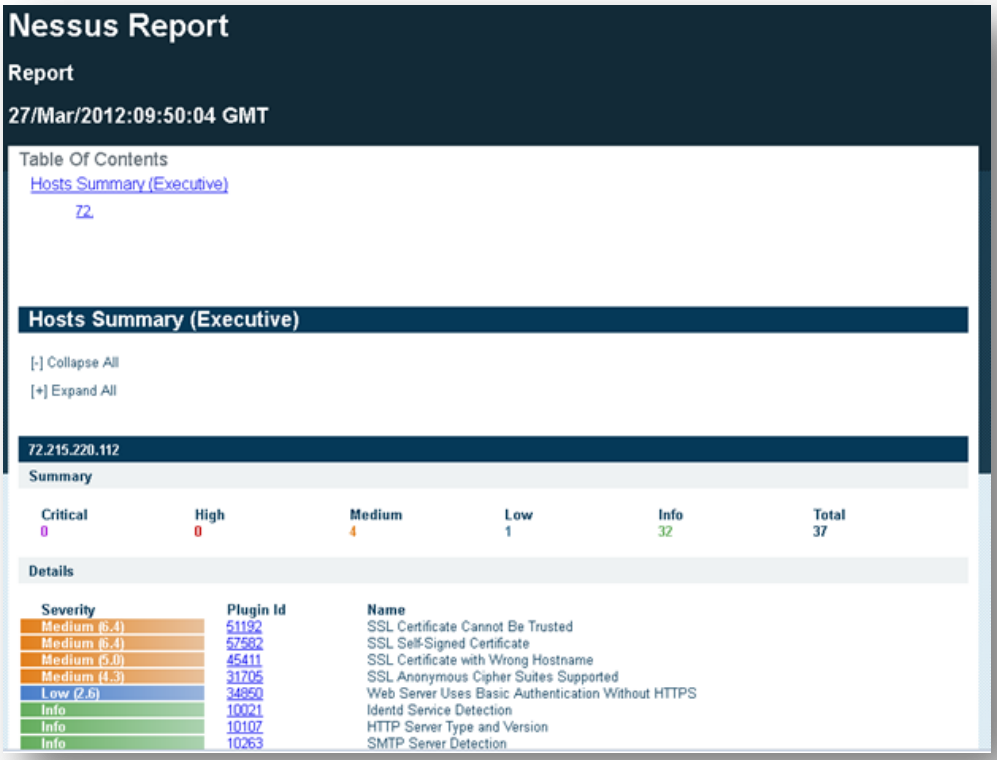

*Análisis finalizado en la vista “Browse” (Explorar)*




*Informe de análisis finalizado seleccionado para descargar*

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





Nessus Report

Report

27/Mar/2012:09:50:04 GMT

Table Of Contents

Hosts Summary (Executive)

72

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

72.215.220.112

Summary

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 4 | 1 | 32 | 37 |

Details

| Severity | Plugin Id | Name |
|---|---|---|
| Medium (6.4) | 51192 | SSL Certificate Cannot Be Trusted |
| Medium (6.4) | 57582 | SSL Self-Signed Certificate |
| Medium (5.0) | 45411 | SSL Certificate with Wrong Hostname |
| Medium (4.3) | 31705 | SSL Anonymous Cipher Suites Supported |
| Low (2.6) | 34850 | Web Server Uses Basic Authentication Without HTTPS |
| Info | 10021 | Identd Service Detection |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10263 | SMTP Server Detection |

*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 PCI ASV

En marzo de 2012 Tenable Network Security, Inc. se convirtió en un Proveedor de análisis aprobado (ASV) de PCI, y está certificado para validar análisis de vulnerabilidades de sistemas con conexión a Internet para comprobar su observancia de determinados aspectos de los PCI Data Security Standards (PCI DSS) (Estándares de seguridad de datos de PCI [PCI DSS]). 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 externas, además de 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 de PCI ASV válido. Los clientes tienen permitidos hasta 2 envíos de informes trimestrales para la validación de PCI ASV a través de Tenable Network Security, Inc.

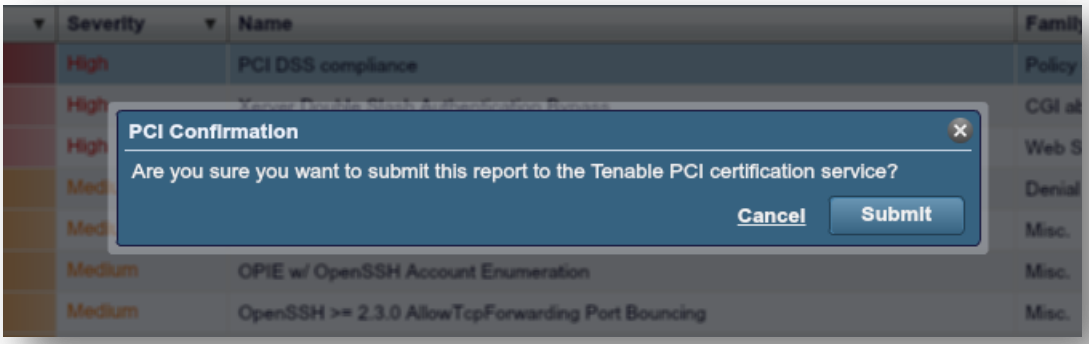
Una vez que iniciaron sesión en el servicio, los clientes tienen la opción de escoger una directiva llamada “PCI DSS”, que cumple con todos los requisitos de la Guía del programa PCI ASV v1.0, sección “ASV Scan Solution – Required Components” (Solución de análisis ASV – Componentes necesarios). Los clientes no tienen la capacidad de alterar ninguno de los parámetros preestablecidos de esta directiva.

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

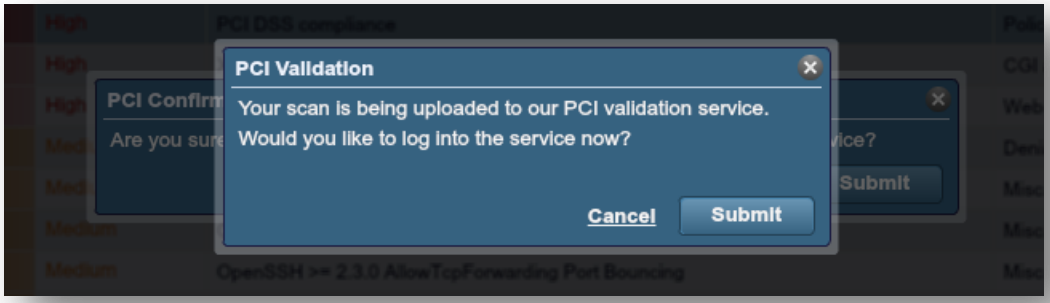

## Envío de resultados de análisis para la revisión del cliente de PCI

Los clientes tienen la opción de enviar los resultados de sus análisis a Tenable Network Security para la validación de PCI ASV. Si hace clic en “Submit for PCI Validation” (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 Validation” (Enviar para validación de PCI)*



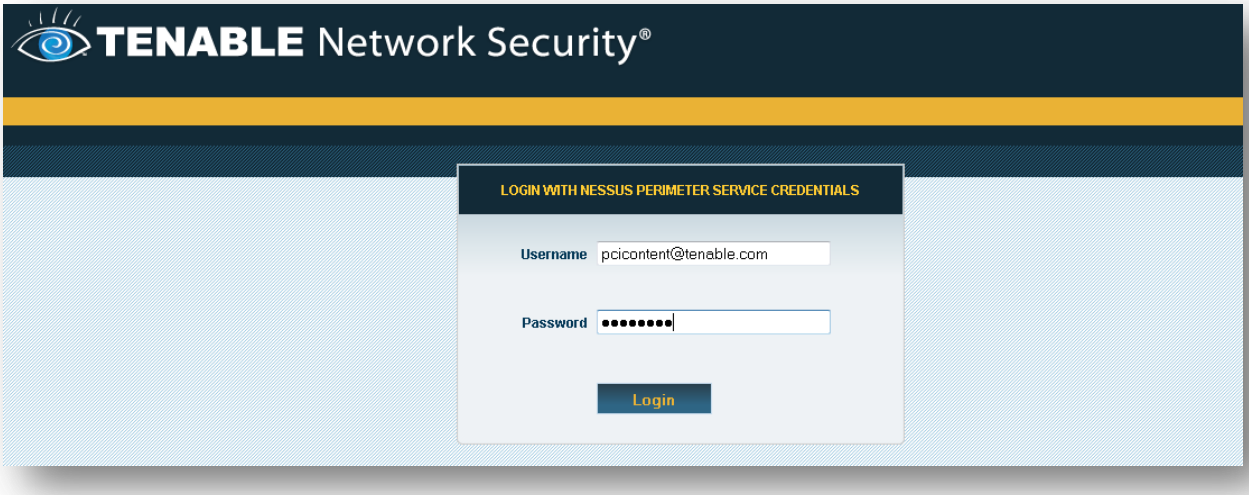

*Cuadro de diálogo de confirmación de envío de informe*




*Cuadro de diálogo de confirmación de carga de informe y de inicio de sesión en el PCI Scanning Service (Servicio de análisis PCI)*

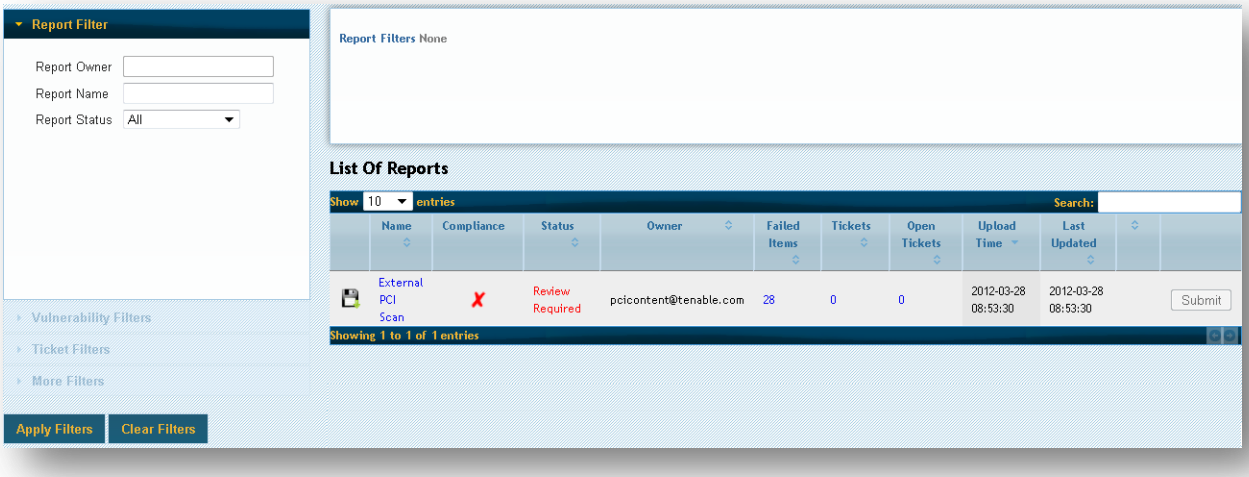
Se les pide encarecidamente a los clientes que revisen exhaustivamente los resultados de sus análisis PCI antes de enviar su(s) informe(s) a Tenable Network Security a través del PCI Scanning Service (Servicio de análisis PCI). Se requiere que los informes con resultados desaprobados atraviesen un ciclo 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 sección de usuarios 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).



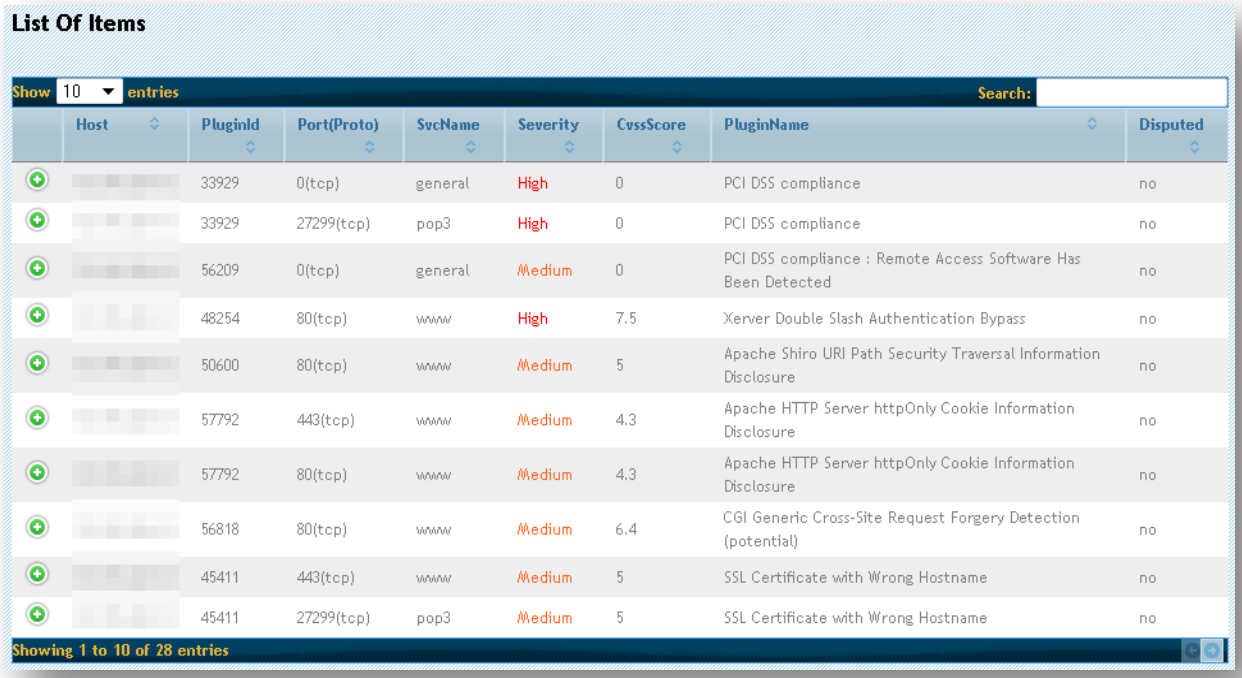

## Revisión de los resultados de un análisis

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 "High" (Alta) o "Medium" (Media) (o con ua 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 "High" (Alta) o "Medium" (Media) en el Nessus Perimeter Service pueden verse en detalle, y todos los elementos tienen una opción para cuestionar.

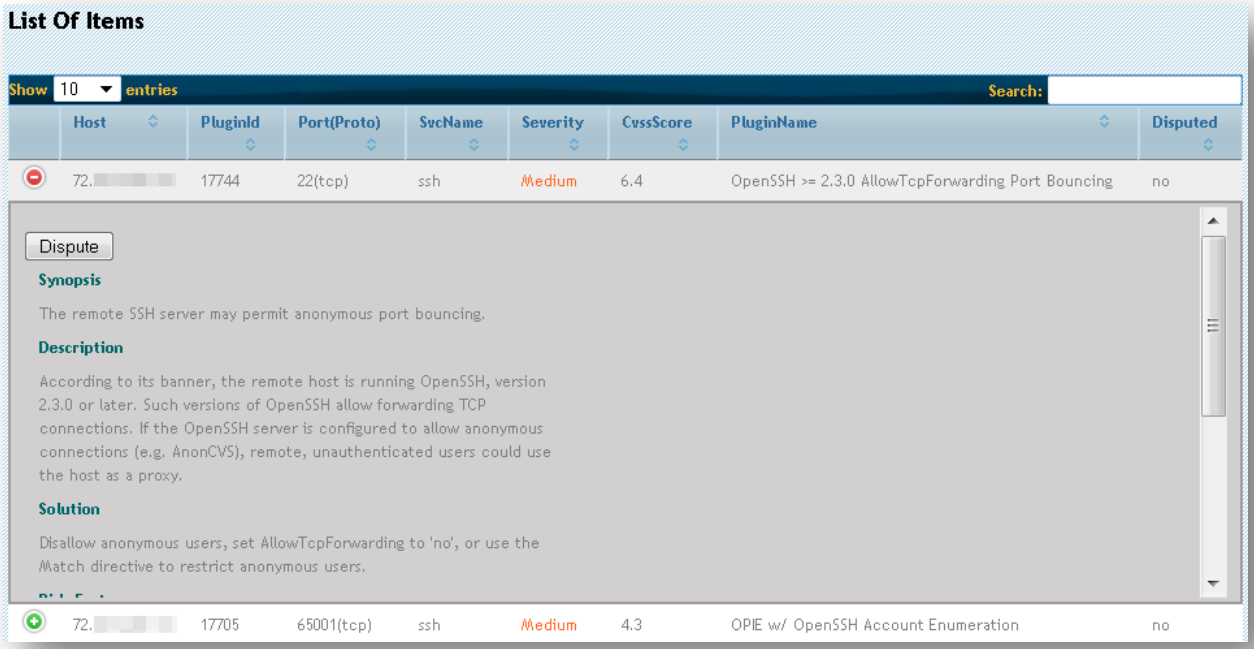
Si hace clic en el nombre del análisis en "List of Reports" (Lista de informes), el usuario puede ver una lista de hosts y la cantidad de vulnerabilidades encontradas en cada host, ordenadas por gravedad.


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 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 PCI ASV.




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

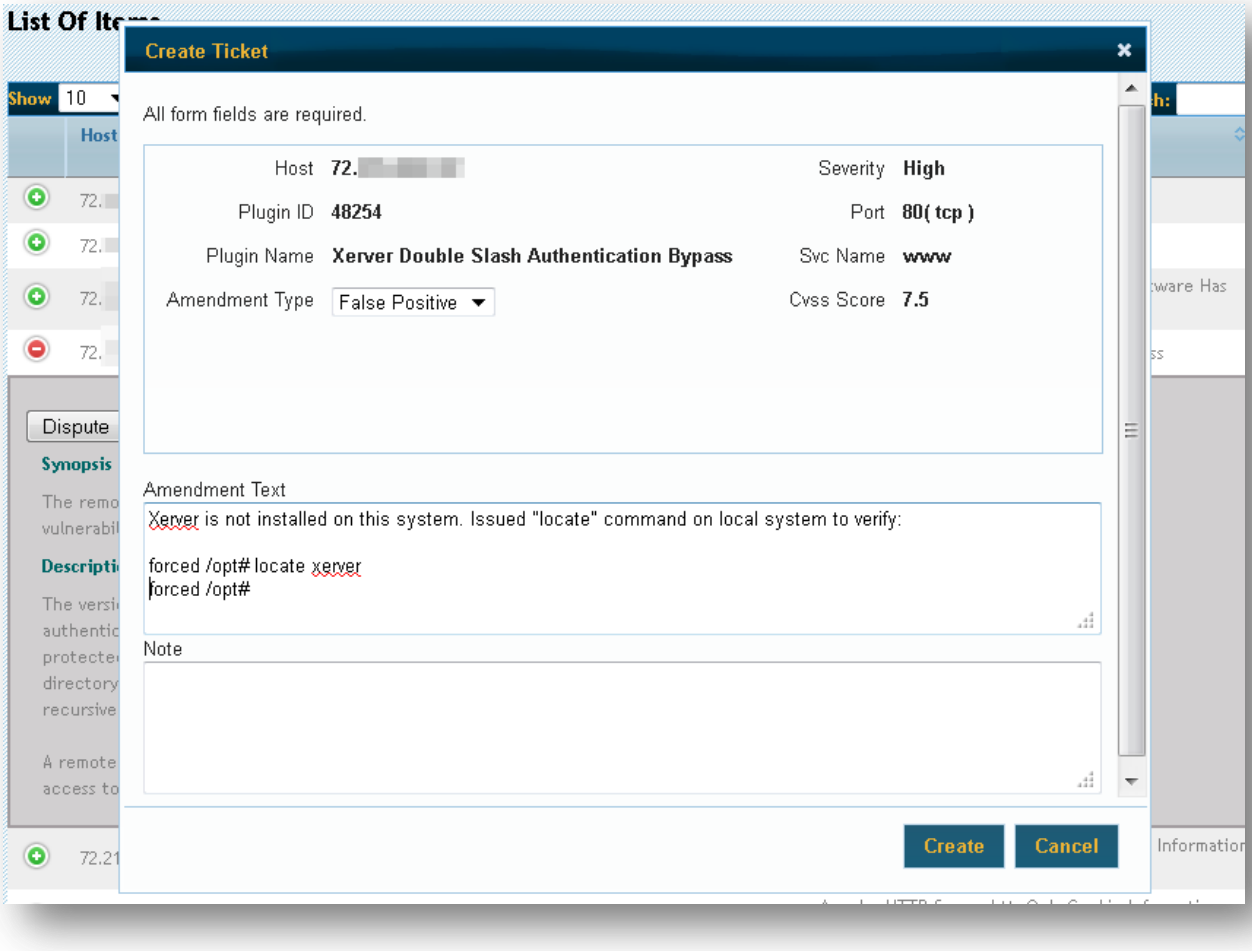



*Descripción del elemento del informe de análisis con la funcionalidad "Dispute" (Cuestionamiento)*

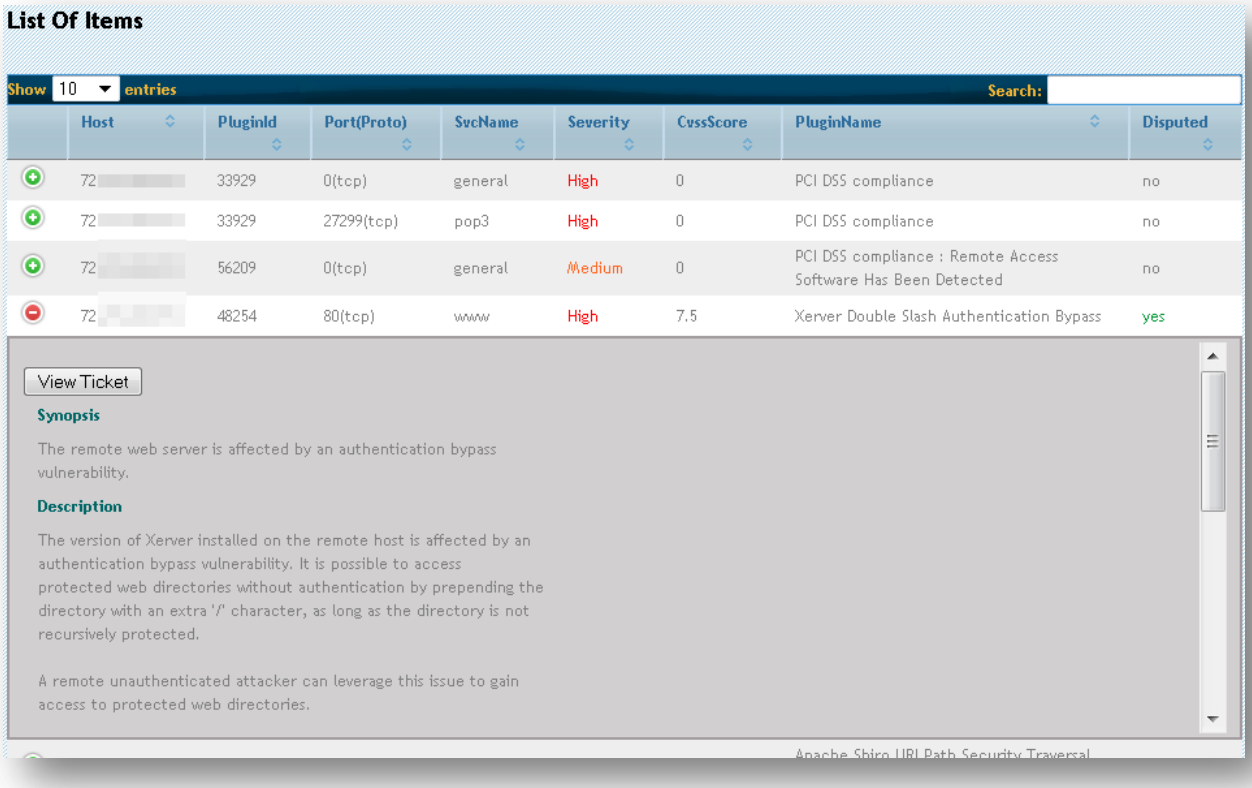
Como se muestra arriba, se visualiza un botón "Dispute" (Cuestionamiento) para cada elemento individual, lo que permite que el cliente introduzca más detalles acerca de la corrección de la vulnerabilidad o que cuestione lo que considera que puede ser un falso positivo generado por el análisis inicial.

## Cuestionamiento de resultados de análisis

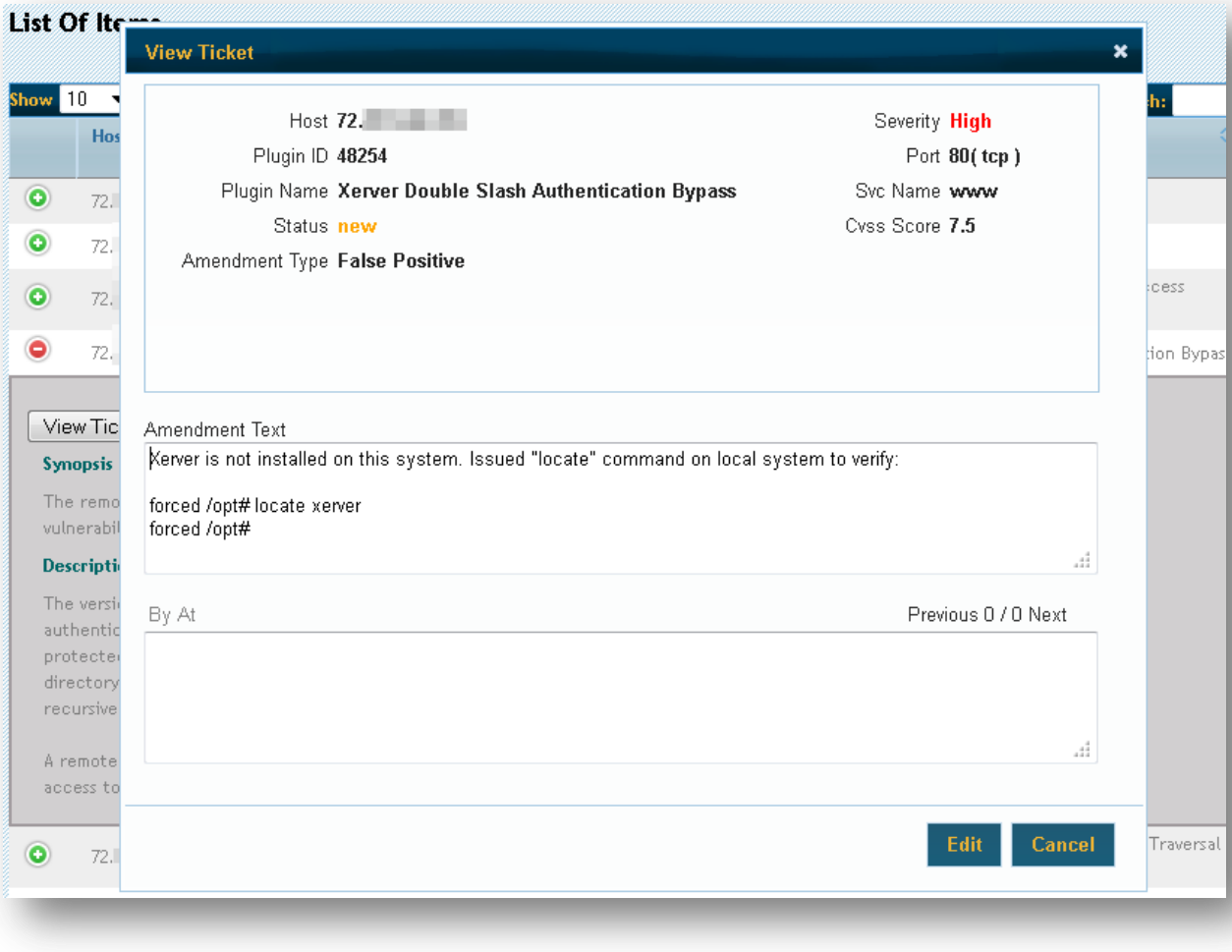
Cuando se cuestiona un elemento, se crea un ticket que permite la selección de un tipo de modificación, el agregado de texto a la modificación, y el agregado de cualquier otro comentario que el cliente quiera hacer antes de enviarlo para la revisión de Tenable Network Security.



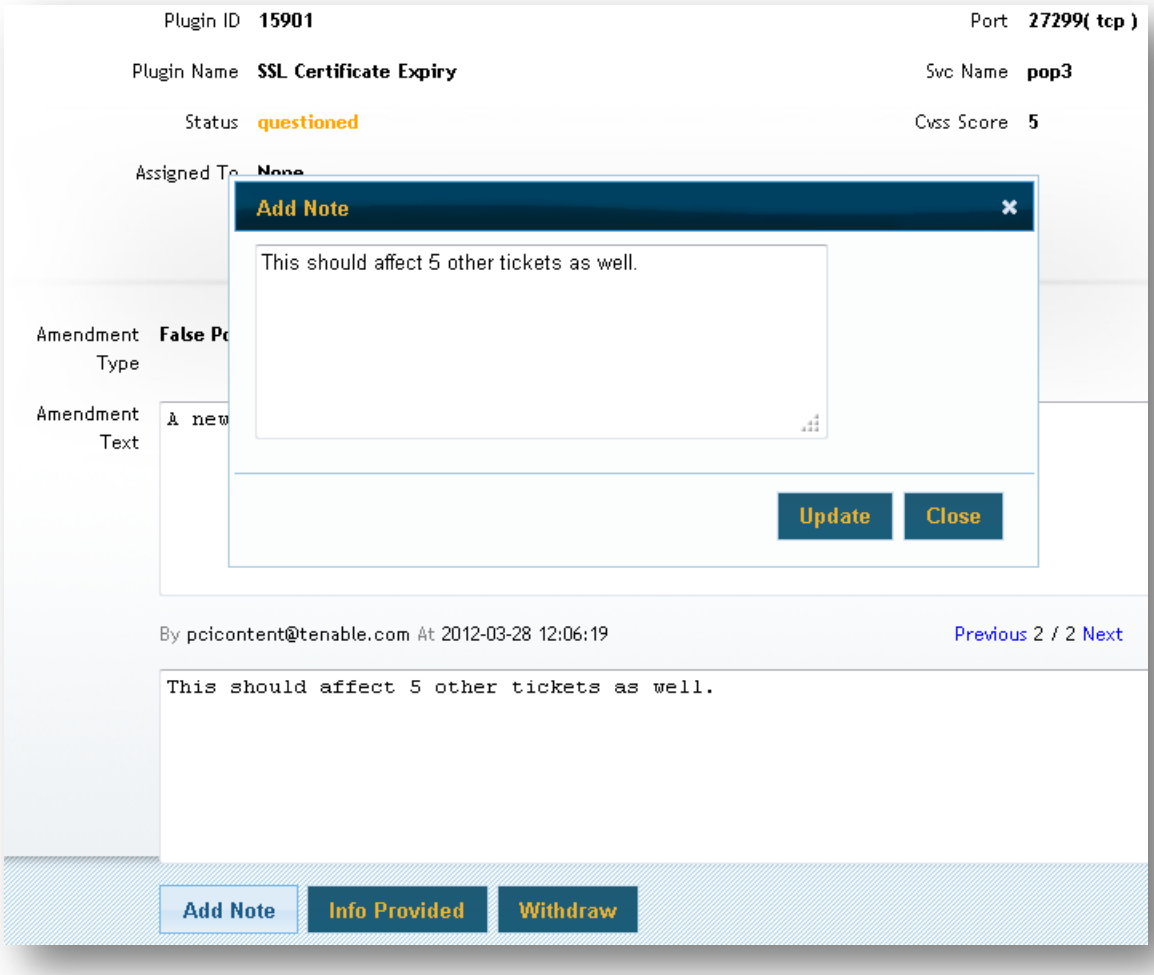

Una vez que se creó un ticket para un elemento específico, el cliente puede verlo seleccionando el elemento en cuestión y haciendo clic en “View Ticket” (Ver ticket).




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



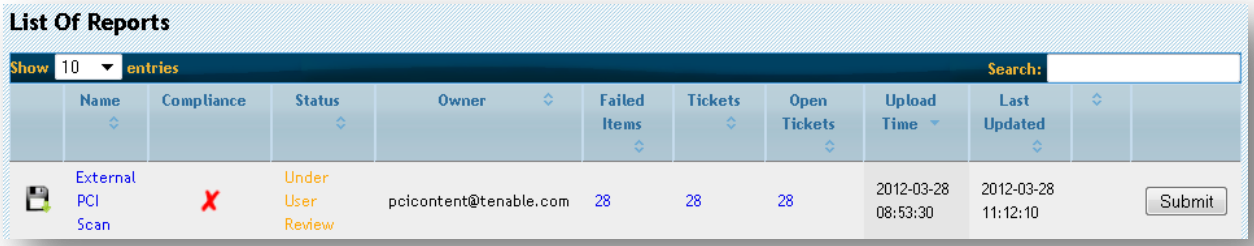

Puede agregar más comentarios haciendo clic en el botón “Edit” (Editar), luego en “Add Note” (Agregar nota), y guardar la nota en el ticket haciendo clic en “Update” (Actualizar).



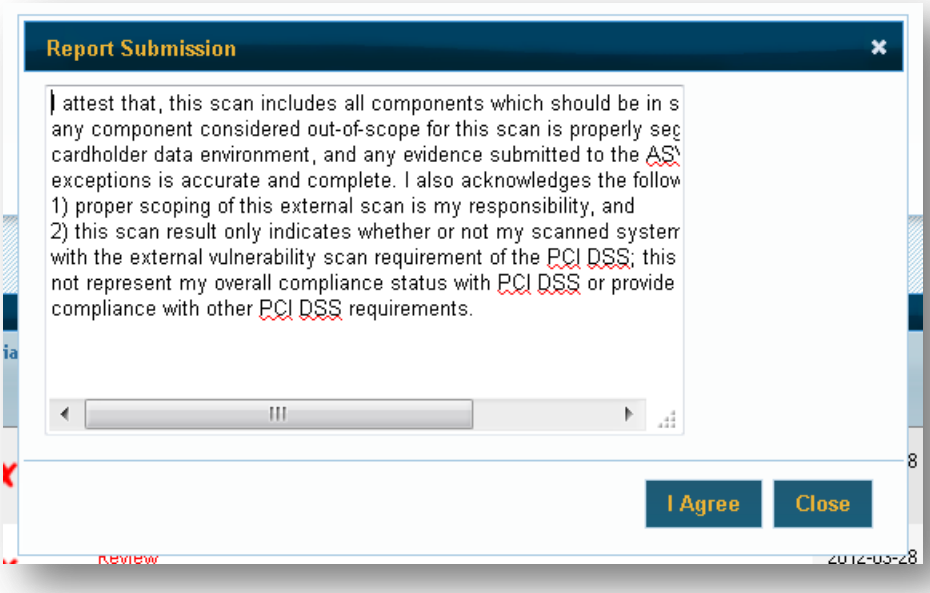

El plugin 33929, “PCI DSS Compliance”, es un plugin administrativo que vincula con los resultados de otros plugins. Si un informe muestra que un host no es compatible con PCI DSS, la resolución de todos elementos que fallan permitirá que se resuelva el plugin 33929 y se reemplace por el plugin 33930,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

## 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.

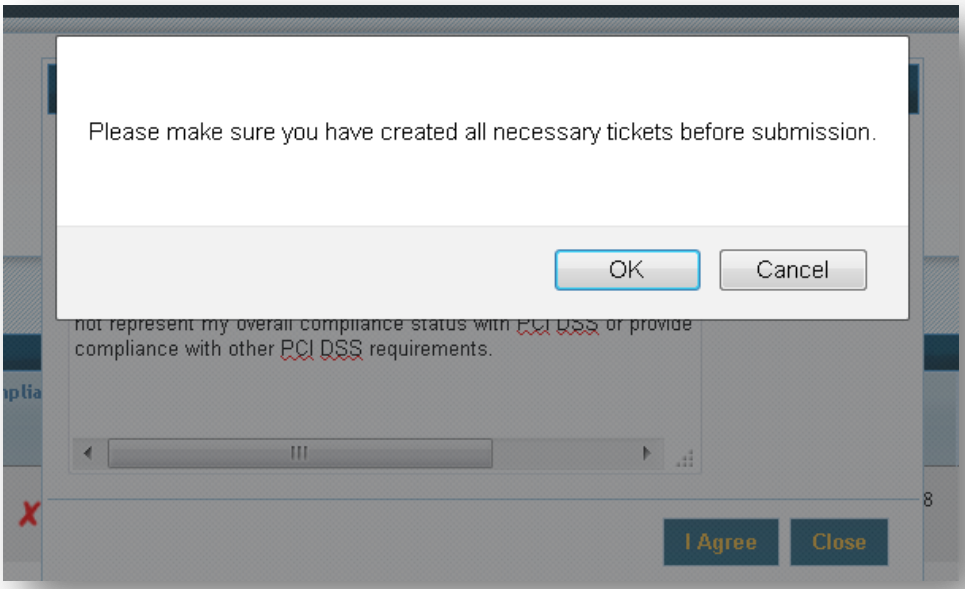



Antes de poder enviar un informe para su revisión, el cliente debe aceptar una declaración que incluye texto obligatorio, según se describe en la Guía del programa de ASV.

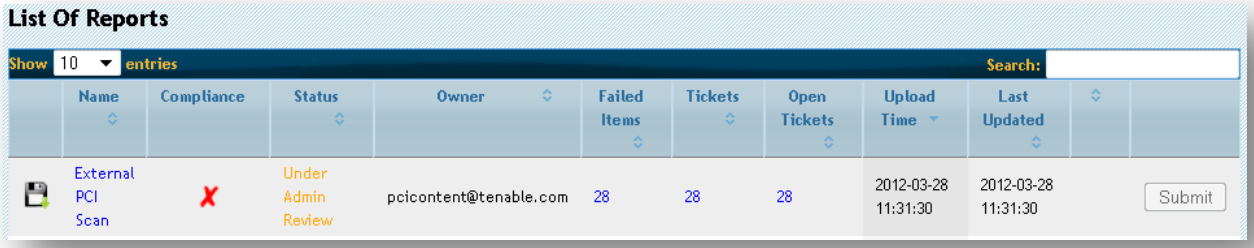



*Texto de declaración de envío de informe*

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.



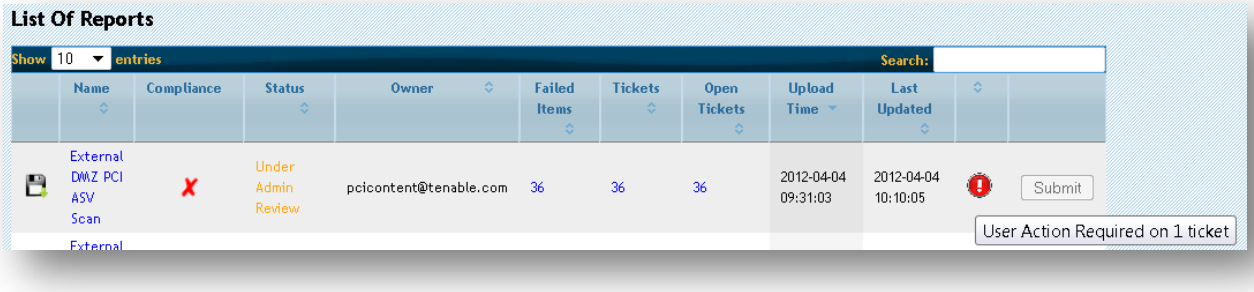

Cuando finalmente se envía un informe a Tenable Network Security para su revisión, el estado del informe cambia de "Under User Review" (En revisión del usuario) a "Under Admin Review" (En revisión del administrador), y la opción "Submit" (Enviar) desaparece para evitar que se envíen elementos o informes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




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

La función "Withdraw" en un ticket abierto sólo está disponible una vez que el informe se haya enviado para la revisión a través del PCI Scanning Service 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:

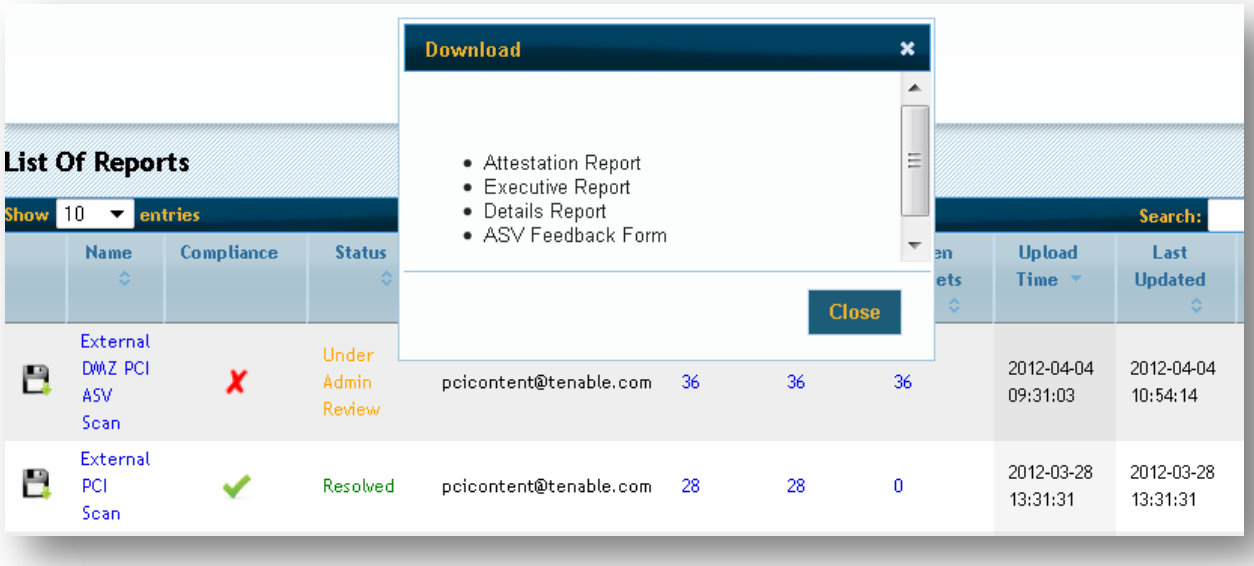



*Notificación “User Action Required” (Se requiere acción del usuario)*

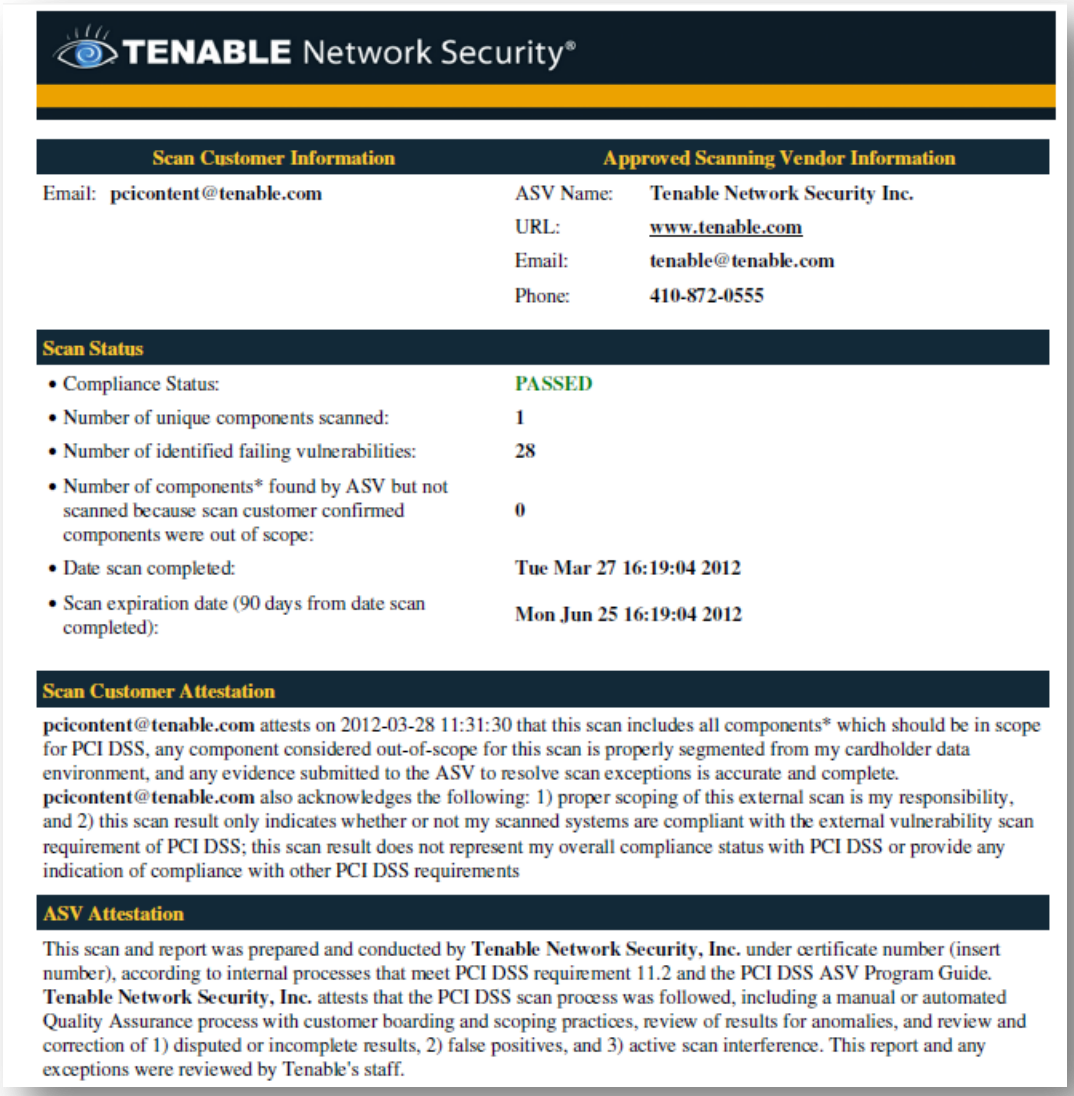
Luego, el usuario puede modificar el ticket y volver a enviarlo a Tenable Network Security para una nueva revisión.

## Formatos de informe de PCI ASV

Una vez que un informe de análisis recibió el estado “compliance” (compatibilidad) del PCI Scanning Service de Tenable, los clientes tienen la opción de ver los informes en los formatos “Attestation Report” (Informe de atestación), “Executive Report” (Informe ejecutivo) o “Detailed Report” (Informe detallado). El cliente del Nessus Perimeter Service recibe también un 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 | |
|---|---|---|
| Email: pcicontent@tenable.com | ASV Name: | Tenable Network Security Inc. |
| | URL: | www.tenable.com |
| | Email: | tenable@tenable.com |
| | Phone: | 410-872-0555 |

**Scan Status**

| | |
|---|---|
| • Compliance Status: | PASSED |
| • Number of unique components scanned: | 1 |
| • Number of identified failing vulnerabilities: | 28 |
| • Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: | 0 |
| • Date scan completed: | Tue Mar 27 16:19:04 2012 |
| • Scan expiration date (90 days from date scan completed): | Mon Jun 25 16:19:04 2012 |

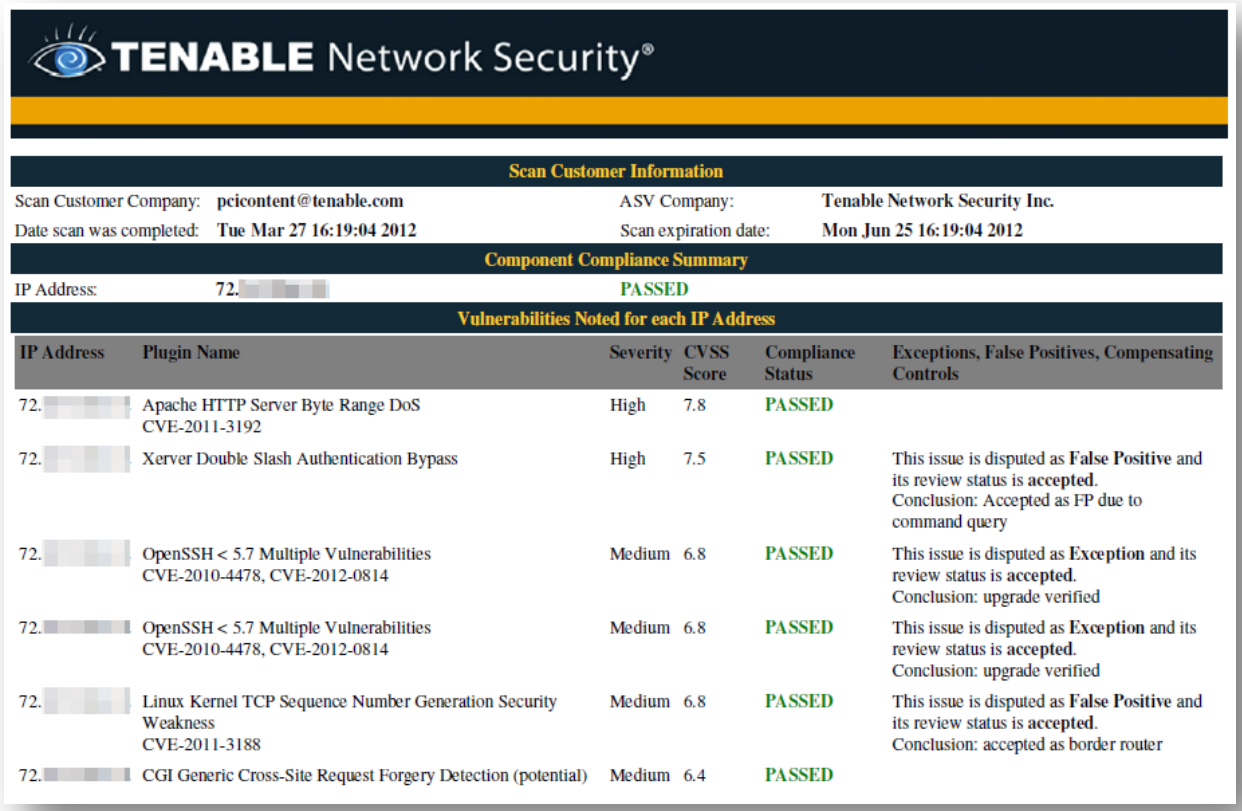
**Scan Customer Attestation**

**pcicontent@tenable.com** attests on 2012-03-28 11:31:30 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. **pcicontent@tenable.com** 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**

This scan and report was prepared and conducted by **Tenable Network Security, Inc.** under certificate number (insert number), 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 Tenable's staff.

*Muestra de informe Attestation Report (Informe de atestación)*



TENABLE Network Security®

**Scan Customer Information**

| | | | |
|---|---|---|---|
| Scan Customer Company: | pcicontent@tenable.com | ASV Company: | Tenable Network Security Inc. |
| Date scan was completed: | Tue Mar 27 16:19:04 2012 | Scan expiration date: | Mon Jun 25 16:19:04 2012 |

**Component Compliance Summary**

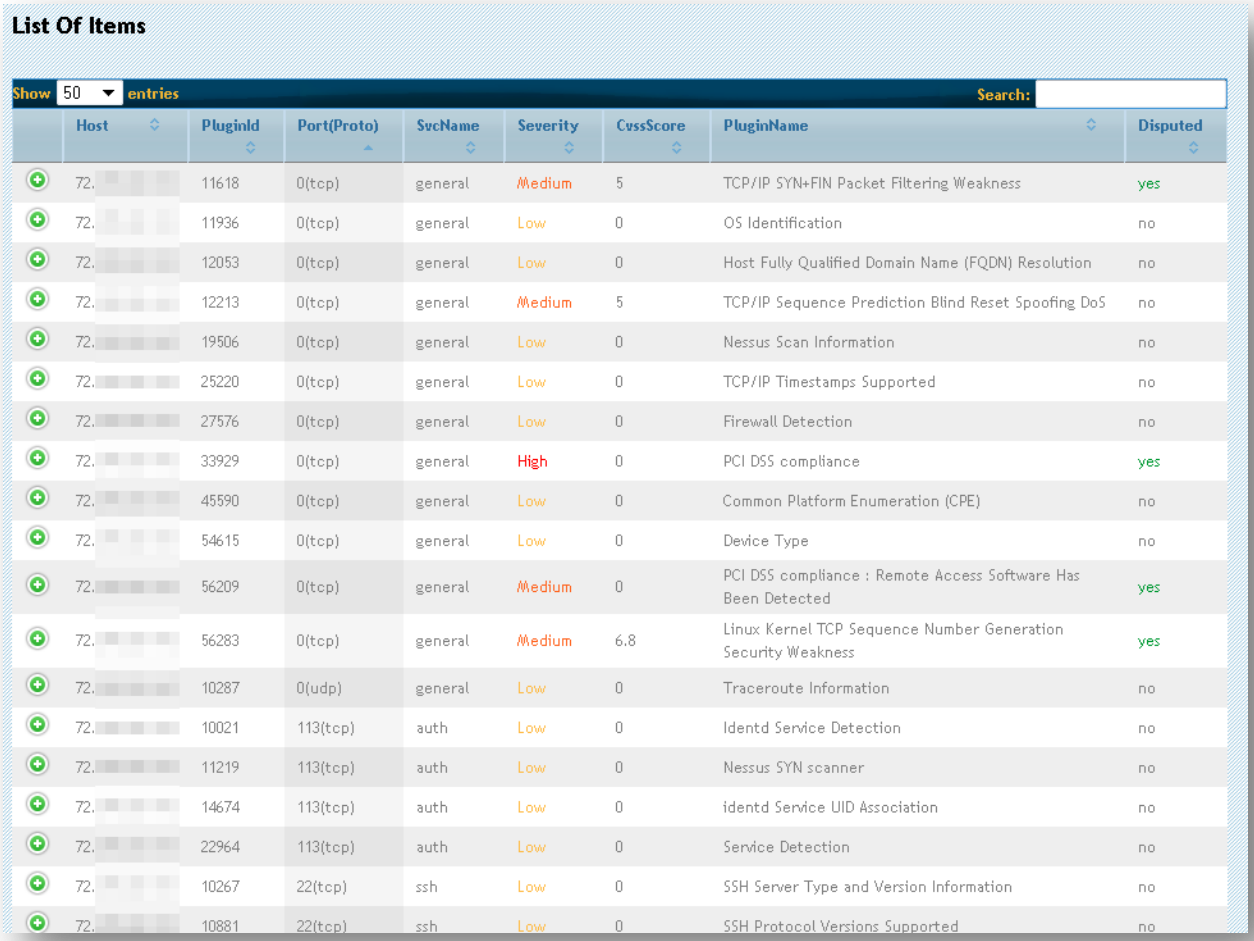
IP Address: 72. PASSED

**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. | Xerver Double Slash Authentication Bypass | High | 7.5 | PASSED | This issue is disputed as **False Positive** and its review status is **accepted**. Conclusion: Accepted as FP due to command query |
| 72. | OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814 | Medium | 6.8 | PASSED | This issue is disputed as **Exception** and its review status is **accepted**. Conclusion: upgrade verified |
| 72. | OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814 | Medium | 6.8 | PASSED | This issue is disputed as **Exception** and its review status is **accepted**. Conclusion: upgrade verified |
| 72. | Linux Kernel TCP Sequence Number Generation Security Weakness CVE-2011-3188 | Medium | 6.8 | PASSED | This issue is disputed as **False Positive** and its review status is **accepted**. Conclusion: accepted as border router |
| 72. | CGI Generic Cross-Site Request Forgery Detection (potential) | Medium | 6.4 | PASSED | |

*Muestra de informe 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 50 entries Search:

| | Host | PluginId | Port(Proto) | SvcName | Severity | CvssScore | PluginName | Disputed |
|---|---|---|---|---|---|---|---|---|
| | 72. | 11618 | 0(tcp) | general | Medium | 5 | TCP/IP SYN+FIN Packet Filtering Weakness | yes |
| | 72. | 11936 | 0(tcp) | general | Low | 0 | OS Identification | no |
| | 72. | 12053 | 0(tcp) | general | Low | 0 | Host Fully Qualified Domain Name (FQDN) Resolution | no |
| | 72. | 12213 | 0(tcp) | general | Medium | 5 | TCP/IP Sequence Prediction Blind Reset Spoofing DoS | no |
| | 72. | 19506 | 0(tcp) | general | Low | 0 | Nessus Scan Information | no |
| | 72. | 25220 | 0(tcp) | general | Low | 0 | TCP/IP Timestamps Supported | no |
| | 72. | 27576 | 0(tcp) | general | Low | 0 | Firewall Detection | no |
| | 72. | 33929 | 0(tcp) | general | High | 0 | PCI DSS compliance | yes |
| | 72. | 45590 | 0(tcp) | general | Low | 0 | Common Platform Enumeration (CPE) | no |
| | 72. | 54615 | 0(tcp) | general | Low | 0 | Device Type | no |
| | 72. | 56209 | 0(tcp) | general | Medium | 0 | PCI DSS compliance : Remote Access Software Has Been Detected | yes |
| | 72. | 56283 | 0(tcp) | general | Medium | 6.8 | Linux Kernel TCP Sequence Number Generation Security Weakness | yes |
| | 72. | 10287 | 0(udp) | general | Low | 0 | Traceroute Information | no |
| | 72. | 10021 | 113(tcp) | auth | Low | 0 | Identd Service Detection | no |
| | 72. | 11219 | 113(tcp) | auth | Low | 0 | Nessus SYN scanner | no |
| | 72. | 14674 | 113(tcp) | auth | Low | 0 | identd Service UID Association | no |
| | 72. | 22964 | 113(tcp) | auth | Low | 0 | Service Detection | no |
| | 72. | 10267 | 22(tcp) | ssh | Low | 0 | SSH Server Type and Version Information | no |
| | 72. | 10881 | 22(tcp) | ssh | Low | 0 | SSH Protocol Versions Supported | no |

*"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/los nombres y la/las direcciones de correo electrónico de la(s) persona(s) de contacto técnico. Se crea automáticamente una cuenta independiente en el Tenable Support Portal para cada Persona de contacto técnico. Las solicitudes de soporte son aceptadas a través del Tenable Support 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.

## Para 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 aquí:

http://www.tenable.com/expert-resources/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 Identificación de cliente con una descripción detallada del problema que experimenta. También puede acceder al Tenable Support Portal para generar un ticket de soporte.

## Acerca de Tenable Network Security

Tenable Network Security, líder en Supervisión de seguridad unificada, es el proveedor del analizador de vulnerabilidades Nessus, y ha creado soluciones de clase empresarial sin agente para la supervisión continua de vulnerabilidades, puntos débiles de configuración, filtración de datos, administración de registros y detección de compromisos para ayudar a garantizar la seguridad de redes y la compatibilidad con FDCC, FISMA, SANS CSIS y PCI. Los galardonados productos de Tenable son utilizados por muchas organizaciones de la lista Forbes Global 2000 y organismos gubernamentales con el fin de minimizar de forma proactiva el riesgo de las redes. Para obtener más información, visite www.tenable.com.


**GLOBAL HEADQUARTERS**

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