

# Guía del usuario de Nessus Perimeter Service (interfaz HTML5)

16 de enero de 2014 (Revisión 5)



# Índice

Introducción	3
Nessus Perimeter Service	3
Suscripción v 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 <u>support@tenable.com</u>.

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 <u>Tenable Store</u> (Tienda de Tenable). Para obtener información sobre los precios, visite la Tienda de Tenable o envíe su consulta a <u>subscriptions@tenable.com</u> 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 <u>licenses@tenable.com</u>. 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:

	<b>Nessus</b> vulnerability scanner	1
>	L Jsername	
	Password	
	Remember Me Sign In	
×	tenable network seetily	$\times$

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 <u>Tenable Support Portal (Portal de soporte de Tenable)</u>.

#### 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.

🕲 Nessus	Scans Schedules Policies		pcicontent@tenable.com 🔻 🗍
Policies			Upload Q Search Policies
New Policy	Policies / All Policies		
All Policies	🗌 Name 🔻	Owner	Туре
Private	PCI-DSS ASV Scan	admin	Shared X
Shared	PCI-DSS ASV Scan (Iow bandwidth)	admin	Shared X
	PCI-DSS ASV Scan (unresponsive hosts)	admin	Shared ★
	Perimeter Scan (exhaustive)	admin	Private 🔀
	Perimeter Scan (fast)	admin	Private 🗙
	Web App Tests	admin	Private 🔀
	Web App Tests (exhaustive)	admin	Private 🗙

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.

Scans		
Scans	New Scan / Basic	Settings
Basic Settings	Name	
Schedule Settings	Policy	External Network Scan
	Folder	my scans 💌
	Targets	Example: 192.168.1.1-129.168.1.25, sample.host.com
	Upload Targets	Add File

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:

🕲 Nessus	Scans 3 Schedules Polici	ies Users		admin 👻 🌅
Schedules			Q Search Schedule	s
New Schedule	Schedules / All Schedules			
All Schedules	Name 🔻	Time	Policy	
	Web App 14 Dev Server	On Demand	Web App Tests	► X
	Weekly Router Scan	On Demand	External Network Scan	► X

#### 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:

Scans			Upload Q Search Scans
New Scan	Scans / My Scans		
My Scans 2	Name	Last Updated 🔺	Status
Trash	DMZ Web Server	October 07, 2013 19:34:48	Completed ×
All Scans	Gateway Internal Scan	October 03, 2013 19:19:22	• Imported ×
New Folder			

#### 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.

Scans			Upload Q Search Scans
🕂 New Scan	Scans / My Scans		
My Scans	Name	Last Updated 🔺	Status
Trash	PCI ASV Scan	May 28, 2013 17:35:26	Completed X
All Scans	PCI ASV Scan	May 28, 2013 10:20:45	Completed ×
New Folder	External DMZ Scan	March 29, 2012 10:00:26	Completed 🗙

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.

( Nessus	<b>PS</b> Scans Schedules	Policies	p @tenable.com ▼ 🙏
External DN	AZ PCI ASV Export •	Audit Trail	Q Filter Vulnerabilities
Scans > Hosts	1 Vulnerabilities 60		Hide Details
Severity 🔺	Plugin Name	Count	Scan Details
HIGH	PCI DSS compliance	2	Name: External DMZ PCI ASV Scan
HIGH	Apache HTTP Server Byte Range DoS	1	Status: Completed
HIGH	Xerver Double Slash Authentication Bypass	1	Policy: PCI-DSS Targets: 72.
MEDIUM	Apache HTTP Server httpOnly Cookie Infor	2	Start time: Tue Apr 10 10:01:08 2012 End time: Tue Apr 10 12:39:56 2012
MEDIUM	OpenSSH < 5.7 Multiple Vulnerabilities	2	Elapsed: 3 hours
MEDIUM	OpenSSH < 5.9 Multiple DoS	2	Vulnerabilities
MEDIUM	OpenSSH >= 2.3.0 AllowTcpForwarding Po	2	Info     Low
MEDIUM	OpenSSH S/KEY Authentication Account En	2	Medium     High     Critical
MEDIUM	OPIE w/ OpenSSH Account Enumeration	2	Cintai
MEDIUM	SSL Anonymous Cipher Suites Supported	2	
-		_	

Análisis finalizado en la vista "Vulnerabilities" (Vulnerabilidades)

Nessus PS	Scans	Schedules	Policies
External DMZ PC	CI ASV	Export 🔻	Audit Trail
Scane > Hosts	Vulnerabilities	Nessus	
	vullerabilities	PDF	
Severity A Plugin	Name	HTML CSV	Count
HIGH PCI DS	S compliance	Nessus DB	2
HIGH Apach	e HTTP Server Byte	e Range DoS	1

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:

Available Content	Report Content
Compliance Check (Executive)	Hosts Summary (Executive)
Suggested Remediations	Vulnerabilities By Host
Vulnerabilities By Plugin 🛛 🚍	
Compliance Check	

Hosts Summary	(Executive)				
[-] Collapse All					
[+] Expand All					
12216-228-112					
Summary					
Critical	High	Medium	Low	Info	Total
0	2	17	3	35	57
Details					
Severity	Plugin Id	Name			
High (7.5)	<u>48254</u>	Xerver Double	Slash Authentication Bypas	55	
High	<u>33929</u>	PCI DSS com	pliance		
Medium (6.8)	<u>44081</u>	OpenSSH < 5	OpenSSH < 5.7 Multiple Vulnerabilities		
Medium (6.4)	<u>17744</u>	OpenSSH >= :	OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing		
	51192	SSL Certificat	e Cannot Be Trusted		
	56818	CGI Generic C	Cross-Site Request Forgery	Detection (potential)	
	<u>57582</u>	SSL Self-Sign	ed Certificate		
Medium (5.0)	12213	TCP/IP Seque	nce Prediction Blind Reset	Spoofing DoS	
	<u>15901</u>	SSL Certificat	e 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".

Policies			Upload Q Search Policies
+ New Policy	Policies / All Policies		
All Policies	Name 🔻	Owner	Туре
Private	PCI-DSS ASV Scan	admin	Shared X
Shared	PCI-DSS ASV Scan (low bandwidth)	admin	Shared X
	PCI-DSS ASV Scan (unresponsive hosts)	admin	Shared 🗙

### 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.

Nessus PS	Scans	Schedules	Policies	
PCI ASV Scan			Export	t   Submit for PCI  Audit Trail
Scans > Hosts	Vulnerabilities 6	Remediations	3 Notes 1	
Host	Vulr	erabilities 🔺		
72.		25	8	67
-	_	_	_	

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

/ulnerabilities 67 Remediations 3 Notes 1	
Vulnerabilities 🔺	Scan
25 8 8 67	Nam
Submit for PCI Validation	×
Are you sure you want to submit this scan for PCI Validation?	if t
Continue Cancel	S

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

tenable network security	
Login with Ne	ssus Perimeter Service credentials
Username	pcicontent@tenable.com
Password	
_	Login

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 <u>PCI Validation user section</u> (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).

eport											
ame											
atus All											
	List	Of Re	ports								
	Shov	10 💌	entries							arch:	
		Name \$	Compliance	Status	\$ Owner 🗘	Failed Items	Tickets \$	Open Tickets \$	Upload Time 🔻	Last 🗘 Updated 🗘	
	8	PCI ASV Scan	×	Review Required	pcicontent@tenable.com	30	0	0	2013-05-21 16:09:35	2013-05-21 16:09:35	Submit
1	Shov	ing 1 to 1	of 1 entries								CO
linerability Filters											

#### 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) o "Medium" (Media) o "Medium" (Media) 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.

	Vuln Filters None	
Vulnerability Filters	More Filters None	
Host Name		
Plugin Id		
Plugin Name	List Of Hosts	
Severity All		
Port	Show 10 🔽 entries Search:	
Protocol	Host Name 🔺 Host IP 🗘 Host FQDN 🗘 Low 🗘 Info 🗘 Medium 🗘 High 🗘	Disputed 🗘
	72. 72. 5 78 28 9 0	
	Showing 1 to 1 of 1 entries	00

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.

w 1	10 💌 entries	Search:							
ŀ	Host 🗢	PluginId \$	Port(Proto)	SvcName	Severity \$	CvssScore \$	PluginName	Dispu	ited
		200012	0(tcp)	general	High	0	pcidss:expired_ssl_certificate	no	
		200001	0(tcp)	general	High	0	pcidss:directory_browsing	no	
		33929	0(tcp)	general	High	0	PCI DSS compliance	no	
		33929	443(tcp)	www	High	0	PCI DSS compliance	no	
		33929	27299(tcp)	рор3	High	0	PCI DSS compliance	no	
		56209	0(tcp)	general	Medium	0	PCI DSS compliance : Remote Access Software Has Been Detected	no	
		57792	443(tcp)	www	Medium	4.3	Apache HTTP Server httpOnly Cookie Information Disclosure	no	
		57792	80(tcp)	www	Medium	4.3	Apache HTTP Server httpOnly Cookie Information Disclosure	no	
		50600	80(tcp)	www	Medium	5	Apache Shiro URI Path Security Traversal Information Disclosure	no	
		56818	80(tcp)	www	Medium	6.4	CGI Generic Cross-Site Request Forgery Detection (potential)	no	

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

Dispute	<b>^</b>
Synopsis	
The remote SSH server may permit anonymous port bouncing.	Ξ
Description	
According to its banner, the remote host is running OpenSSH, version 2.3.0 or later. Such versions of OpenSSH allow forwarding TCP connections. If the OpenSSH server is configured to allow anonymous connections (e.g. AnonCVS), remote, unauthenticated users could use the host as a proxy.	
Solution	
Disallow anonymous users, set AllowTcpForwarding to 'no', or use the Match directive to restrict anonymous users.	Ŧ
wing 1 to 10 of 30 entries	00

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.

Host	72.	Severity	Medium
Plugin ID	50600	Port	80( tcp )
Plugin Name	Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
Amendment Type	False Positive 💌	Cvss Score	5
endment Text ache <u>Shiro</u> is not	installed on the system. Issued "locate" comman	d on the local syst	em to verify:
nendment Text Dache <u>Shiro</u> is not i rced /opt# locate rced /opt#	installed on the system. Issued "locate" comman <u>shiro</u>	d on the local syst	em to verify: //
nendment Text pache <u>Shiro</u> is not i rced /opt# locate rced /opt#	installed on the system. Issued "locate" comman <u>shiro</u>	d on the local syst	em to verify:

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).

st Of Items							
ow 10 💌 entrie	5					Search:	
Host 🗘	PluginId \$	Port(Proto)	SvcName \$	Severity \$	CvssScore \$	PluginName	<ul> <li>Disputed</li> </ul>
72.	50600	80(tcp)	www	Medium	5	Apache Shiro URI Path Security Traversal Information Disclosure	yes
View Ticket Synopsis The remote web ser affected by an infor Description	ver appears mation disc	to use a secu losure vulnera	rity framewo ability,	ork that is			III
The remote web ser source security fram paths before compa file.	ver appears ework that ring them t	to be using a that does not o entries in th	version of t : properly no ie framewor	he Shiro ope ormalize URI k's 'shiro.ini'	n		
A remote attacker c: authorization, or oth crafted requests.	an leverage ier types of	this issue to b security restri	oypass autho ictions via sp	entication, pecially			Ŧ

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

	ost <b>72</b> .	Severity	Medium
) Plugin	ID 50600	Port	80( tcp )
ost Plugin Nar	ne Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
2. Stat	us new	Cvss Score	5
Amendment Ty	pe False Positive		
Fick			
sis			
mo Amendment Text			
3a b			
Apache Shiro is n	ot installed on the system. Issued "locate" command	on the local system	to verify:
Apache Shiro is ni iptii forced /opt# loca	ot installed on the system. Issued "locate" command te shiro	on the local system	to verify:
Apache Shiro is n ipti mo forced /opt# loca forced /opt#	ot installed on the system. Issued "locate" command	on the local system	to verify:
Apache Shiro is n iptic forced /opt# loca forced /opt#	ot installed on the system. Issued "locate" command	on the local system	to verify:
Apache Shiro is n forced /opt# loca forced /opt# forced /opt#	ot installed on the system. Issued "locate" command	on the local system	to verify: // Previous 0 / 0 Next
Apache Shiro is n forced /opt# loca forced /opt# bef( By At pte	ot installed on the system. Issued "locate" command	on the local system	to verify: // Previous 0 / 0 Next
Apache Shiro is n forced /opt# loca forced /opt# befc By At ote izat frei	ot installed on the system. Issued "locate" command	on the local system	to verify: //
Apache Shiro is ni forced /opt# loca forced /opt# bef( By At tree	ot installed on the system. Issued "locate" command	on the local system	to verify: // Previous 0 / 0 Next
Apache Shiro is ni forced /opt# loca forced /opt# befo By At 2.	ot installed on the system. Issued "locate" command	on the local system	to verify: // Previous 0 / 0 Next

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).

	.1050		ocvency	
F	Plugin ID	15901	Port	443( tcp )
Plug	in Name	SSL Certificate Expiry	Svc Name	www
	Statu	Add Note	×	
Assi	gned T	This should affect 5 other tickets as well.		
Amendment Type	False		11	
Amendment Text	Thi:		Update Close	
	By At		Previ	ous 0 / 0 Next
				//



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:

	Name \$	Compliance	Status	\$ Owner 🗢	Failed Items	Tickets \$	Open Tickets	Upload Time 👻	Last Updated \$	\$
P	PCI ASV Scan	×	Under User Review	pcicontent@tenable.com	30	1	1	2013-10-11 15:33:52	2013-10-11 15:35:54	Submit

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

Show 10 🔻 entries							Search:
Report Name 🔺	Host Name 🗢	Port ᅌ	Plugin ᅌ	Severity 💠	Cvss Score 🗢	Status ᅌ	Assigned To 💠 Last Updated 🗢
PCI ASV Scan	72.	80(tcp)	50600	Medium	5	new	2013-10-11 15:35:54
Showing 1 to 1 of 1 entr	ries						

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

	Host	72.	Severity	Medium
PI	lugin ID	50600	Port	80(tcp)
Plugir	n Name	Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
	Status	new	Cvss Score	5
Assig	gned To	None	Attachments	None
Uplo	oad File:	Browse No file selected.	Attach	
Amendment Type	False P	ositive		
Amendment Text	The s	server is not running Shiro		

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:

	Host	72.	Severity	Medium
PI	ugin ID	50600	Port	80(tcp)
Plugir	n Name	Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
	Status	new	Cvss Score	5
Assig	gned To	None	Attachments	Download
Uplo	ad File:	Browse no_shiro.png	Attach	The file was uploaded successfully!
Amendment Type	False Po	ositive		
Amendment Text	The s	erver is not running Shiro		

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.

10W	10 💌	entries						Sea	arch:	
	Name \$	Compliance	Status ᅌ	Owner 💠	Failed Items	Tickets \$	Open Tickets ᅌ	Upload Time 🔻	Last Updated ≎	\$
8	PCI ASV Scan	×	Under User Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 08:57:44	Submit
lowi	ng 1 to 1	of 1 entries								GO

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).

Contact Name:	John Smith		ſ
Company:	Tenable Network Security Jo	b PCI Analyst e:	
Phone:	(410) 872-0555		=
Address:	7063 Columbia Gateway Dr		
City:	Columbia State	e: MD	
ZIP:	21046		
URL:	http://www.tenable.com		-

Report Submission	×
I attest 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. I 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 the 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.	
Previous I Agree	e Close

#### 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.

#### List Of Reports

iow	10 💌	entries						Sea	arch:	
	Name \$	Compliance	Status 💠	Owner 🗢	Failed Items	Tickets \$	Open Tickets ᅌ	Upload Time	Last Updated ≎	\$
8	PCI ASV Scan	x	Under User Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 08:57:44	Submit

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.

w	10 💌	entries						Sea	arch:		
	Name \$	Compliance	Status 💠	Owner 💠	Failed Items	Tickets \$	Open Tickets \$	Upload Time 🔻	Last Updated ≎	٥	
	PCI ASV Scan	×	Under Admin Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 09:18:21		Submit
wi	ng 1 to 1 (	of 1 entries									OC

#### 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:

#### List Of Reports

Name \$	Compliance	Status 💠	Owner 🗘	Failed Items	Tickets \$	Open Tickets	Upload Time	Last Updated ᅌ	\$		
PCI ASV	x	Under Admin Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 10:43:31	0	Submit	

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.



	Scan Customer Information	Aj	pproved 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 0 scope:
- Date scan completed:



• 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



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)



		See Createrne Informer	49		
		Scan Customer Informa	tion		
Scan Customer Co	mpany: Tenable Network Security	ASV Com	ipany:	Tenable Netv	vork Security
Date scan was com	pleted: Tue May 21 12:39:34 2013	Scan expir	ration date:	Mon Aug 19	12:39:34 2013
		Component Compliance Su	mmary		
IP Address:	72.1	PASSED			
	,	Vulnerabilities Noted for each l	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	<ul> <li>Disputed</li> <li>Image: Image of the second sec</li></ul>		
0	72.		17704	65001(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes		
0	72.		17704	22(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes		
0	72.		53841	65001(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no		
0	72.		53841	22(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no		
0	72.		17703	65001(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no		
0	72.		17703	22(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no		
0	72.		17705	65001(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes		
0	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		
0	72.		44081	22(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes		

# 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 <u>support@tenable.com</u>. 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.

Nessus PS	Scans	Schedules	Policies		@tenablesecurity.com	-	Ļ

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 <u>www.tenable.com</u>.

#### SEDE CENTRAL MUNDIAL

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

