TENABLE NESSUS EXPERT

El estándar de oro para la evaluación de vulnerabilidades

Debido a los recursos escasos, el tiempo limitado y una superficie de ataque en constante cambio, a los profesionales de la seguridad de vanguardia les resulta difícil seguirles el ritmo a los agentes maliciosos. Lo que se necesita es una forma rápida y sencilla de descubrir, priorizar y corregir vulnerabilidades de forma proactiva. Lo que se necesita es Tenable Nessus® Expert.

Nessus Expert automatiza las evaluaciones en un momento dado para ayudarlo a identificar y corregir con rapidez las vulnerabilidades, incluyendo parches faltantes, defectos de software, malware y configuraciones erróneas, en diversos sistemas operativos, dispositivos y aplicaciones.

La superficie de ataque moderna en evolución

Cuando Nessus se introdujo en 1998 como la primera herramienta de evaluación de vulnerabilidades (VA) de la industria, la superficie de ataque estaba compuesta por dispositivos informáticos tradicionales: computadoras de escritorio, estaciones de trabajo, equipos en red, etc. Sin embargo, a medida que fueron surgiendo nuevas tecnologías a lo largo de los años, la superficie de ataque moderna se amplió y los agentes maliciosos están aprovechando eso.

Están surgiendo nuevos vectores de ataque que van mucho más allá de los activos de TI convencionales y que hay que defender. Los atacantes han explotado vulnerabilidades en áreas como la infraestructura en la nube, la superficie de ataque externa y las aplicaciones web para infiltrarse en innumerables redes. Los profesionales de la seguridad, consultores, desarrolladores y evaluadores de penetración necesitan una única solución de evaluación de vulnerabilidades que aborde tanto las amenazas convencionales como las que están vinculadas con la superficie de ataque moderna.

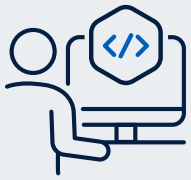
Cobertura amplia y completa

Tenable Research trabaja estrechamente con la comunidad de seguridad para detectar nuevas vulnerabilidades y proporcionar información, a fin de ayudar a las organizaciones a lograr prácticas más maduras de evaluación de vulnerabilidades. El equipo de vulnerabilidades de día cero de Tenable ha detectado más de 465 vulnerabilidades de día cero desde 2019.

Una adición al kit de herramientas de evaluación

Nessus es el escáner de vulnerabilidades más reconocido de la industria porque proporciona una visibilidad inigualable hacia las vulnerabilidades, los errores de configuración y las condiciones de incumplimiento asociadas con sus activos de TI convencionales. Nessus Expert se suma a esa tradición al brindar la misma visibilidad hacia la superficie de ataque moderna que incluye sus activos accesibles desde Internet, infraestructura en la nube y aplicaciones web, todo bajo un mismo techo.

Detecte y evalúe sus activos de TI



Fortalezca sus aplicaciones web

Proteja la infraestructura en la nube antes de la implementación

Vea la superficie de ataque accesible desde Internet

NESSUS EXPERT Y LA SUPERFICIE DE ATAQUE MODERNA

Aceleración de la detección (shift left) y protección de la infraestructura en la nube

Gracias a los servicios y las infraestructuras en la nube, implementar nuevas aplicaciones y cargas de trabajo resulta sencillo. Sin embargo, la velocidad y la agilidad conllevan riesgos cibernéticos adicionales y desconocidos dentro de esos entornos. Existen soluciones que están diseñadas para proteger la nube, pero se aplican demasiado tarde. Nessus Expert le permite escanear sus repositorios de código de Infrastructure as Code (IaC) en busca de deficiencias de seguridad antes de enviarlos a producción para evitar riesgos desconocidos.

BENEFICIOS PRINCIPALES:

- Tener un abordaje proactivo con respecto a la evaluación de vulnerabilidades de las cargas de trabajo en la nube.
- Escanear en busca de vulnerabilidades problemáticas y costosas antes de implementar el código.
- Aprovechar 500 políticas prediseñadas para escanear la IaC.
- Evitar que los errores de configuración y las vulnerabilidades lleguen a las instancias de producción en la nube.

Obtenga visibilidad hacia su superficie de ataque accesible desde Internet

La superficie de ataque moderna está compuesta por activos accesibles desde Internet que suelen ser desconocidos debido a la falta de controles de inventario y a la capacidad de los desarrolladores de poner en marcha instancias en la nube en cuestión de minutos. Desde el punto de vista de un atacante, los activos accesibles desde Internet proporcionan una forma sencilla pero sigilosa de sondear las vulnerabilidades e infiltrarse en una red, especialmente si ni siquiera se sabe que existen. Nessus Expert le permite detectar y evaluar estos activos desconocidos en busca de vulnerabilidades, errores de configuración y condiciones de incumplimiento.

BENEFICIOS PRINCIPALES:

- Detectar activos conectados a Internet que antes eran desconocidos para la organización.
- Iniciar escaneos de evaluación de los activos de reciente identificación.
- Escanear hasta cinco dominios cada 90 días para comprender todos los subdominios con los que están asociados.
- Crear un inventario constante de sus activos conectados a Internet.
- Comprender el riesgo y cerrar la brecha de los activos fuera de su perímetro.

Análisis de varios niveles para fortalecer sus aplicaciones web

La aplicación web promedio tiene entre 3 y 5 vulnerabilidades, incluyendo muchas de gravedad elevada. Con casi 2 mil millones de aplicaciones web en el mundo, no sorprende que estas sigan siendo uno de los vectores de ataque más comunes que generan filtraciones de datos. El escaneo de aplicaciones web en Nessus Expert proporciona una funcionalidad de prueba de seguridad de aplicaciones dinámicas (DAST) que brinda visibilidad e información completas sobre los problemas de seguridad de las aplicaciones web. Escanea de forma segura aplicaciones web modernas e identifica con precisión vulnerabilidades en el código personalizado de la aplicación, así como versiones vulnerables de componentes de terceros que constituyen la mayor parte de la aplicación.

BENEFICIOS PRINCIPALES:

- Admite cinco nombres de dominio totalmente calificados (FQDN) con la opción de agregar más.
- Configure fácilmente nuevas aplicaciones web y escaneos de API, y genere resultados completos.
- Identifique vulnerabilidades tanto en el código personalizado de su aplicación como en los componentes web que lo respaldan.
- Identifique rápidamente problemas de higiene cibernética de aplicaciones web relacionados con certificados SSL/TLS y errores de configuración de los encabezados HTTP.
- Escanee entornos con confianza y seguridad sin sufrir interrupciones ni retrasos.
- Creado y respaldado por Tenable Research, el número uno en cobertura y precisión de vulnerabilidades.

Nessus es la solución n.º 1 de evaluación de vulnerabilidades

N.º 1 en exactitud

Nessus tiene el índice de falsos positivos más bajo de la industria con una precisión de seis sigma (medido en 0,32 defectos por 1 millón de escaneos).

N.º 1 en cobertura

Nessus tiene la cobertura más amplia y completa, con más de 77 000 CVE y el lanzamiento de más de 100 nuevos plug-ins cada semana dentro de las 24 horas de la revelación de vulnerabilidades.

N.º 1 en adopción

Más de 30 000 organizaciones de todo el mundo confían en Nessus, incluyendo 2 millones de descargas. El 50 % de las compañías de la lista de Fortune 500 y más del 30 % de las compañías de la lista Global 2000 confían en la tecnología Nessus.

Aproveche el poder de la priorización predictiva

Aproveche el Índice de Priorización de Vulnerabilidades (Vulnerability Priority Rating, VPR) de Tenable para concentrarse en las vulnerabilidades que representan el mayor riesgo para su entorno y corregirlas primero. El VPR se genera al combinar datos de vulnerabilidades de Tenable y de terceros con datos de amenazas externas y analizarlos con un algoritmo avanzado de ciencia de datos desarrollado por Tenable Research.

POR QUÉ NESSUS DIRIGE EL CAMINO

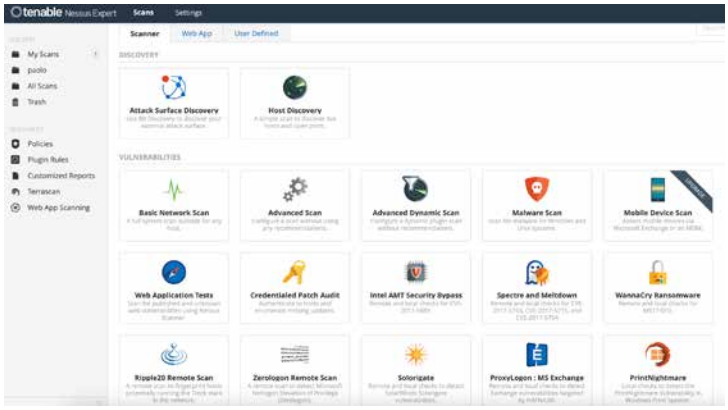
Facilidad de uso

Diseñado por profesionales de la seguridad para profesionales de la seguridad, Nessus se desarrolló con el único propósito de brindar una experiencia intuitiva para que los profesionales de la seguridad de vanguardia puedan descubrir y corregir las vulnerabilidades más rápido y con más confianza.

Las actualizaciones de la experiencia de usuario han hecho que la navegación y la experiencia del usuario sean más fáciles e intuitivas. El nuevo centro de recursos de Nessus ofrece a los usuarios la información pertinente al alcance de su mano. Las guías específicas para el usuario proporcionan consejos prácticos y orientación basados en las operaciones y funciones que se realizan.

Vea rápidamente las vulnerabilidades con políticas y plantillas desarrolladas previamente

Las plantillas de escaneo preconfiguradas y listas para usar le ayudan a comprender rápidamente dónde están las vulnerabilidades, los errores de configuración y las condiciones de cumplimiento. Se proporcionan plantillas de escaneo para activos móviles y de TI, infraestructura en la nube, superficie de ataque externa y aplicaciones web.



Más de 450 plantillas de cumplimiento y configuración le permiten auditar el cumplimiento de la configuración respecto de los análisis comparativos de CIS y otras prácticas recomendadas.

Valor que excede las vulnerabilidades

Si bien Nessus es la configuración de base para las evaluaciones de vulnerabilidades, el valor que proporciona no termina allí. Nessus Expert puede servir para ofrecer servicios adicionales a las organizaciones a fin de aumentar sus percepciones sobre los riesgos. Estos incluyen los siguientes:

Detección de activos: mantenga una lista de inventario actualizada de todos los activos de software, hardware y en la nube en un entorno.

Auditorías de sistema operativo/base de datos/ aplicaciones e infraestructura de red: asegúrese de que los activos de TI cumplan con más de 428 políticas y estándares diferentes.

Auditorías de marcos de seguridad/estándares de cumplimiento: asegúrese de que la configuración y los ajustes administrativos sean seguros y cumplan con los requisitos internos o reglamentarios, los estándares del marco de seguridad y las prácticas recomendadas.

Verificaciones de Active Directory (AD): aproveche 10 verificaciones de AD fundamentales para detectar deficiencias explotadas con frecuencia para ayudar a proteger las credenciales, evitar la escalación de privilegios y prevenir el movimiento lateral.

Sistema operativo y software de terceros no compatibles: identifique rápidamente los sistemas operativos y las aplicaciones que no son compatibles o que están al final de su vida útil (EOL) y que ponen en riesgo a las organizaciones.

Control de cambios y versiones: establezca y marque cambios de versión o desvíos de la "imagen maestra" aprobada para servidores y puntos de conexión.

Auditar activos en la nube: audite activos en entornos de AWS, GCP, Azure, SFDC, Rackspace y Zoom para detectar errores de configuración al nivel de cuenta y/o todos los activos en la nube de un dominio en particular.

Integración: mejore su seguridad operativa y sus percepciones integrando los resultados del escaneo de Nessus en diversas soluciones de seguridad y TI de terceros.

Acerca de Tenable

Tenable® es la empresa de Exposure Management. Aproximadamente 43 000 organizaciones de todo el mundo confían en que Tenable ayuda a comprender el riesgo cibernético y a reducirlo. Como creador de Nessus®, Tenable amplió su conocimiento sobre vulnerabilidades para ofrecer la primera plataforma del mundo para ver y proteger los activos digitales en cualquier plataforma de cómputo. Entre los clientes de Tenable, se incluye aproximadamente al 60 % de las compañías de la lista Fortune 500, aproximadamente el 40 % de las compañías de la lista Global 2000 y grandes instituciones gubernamentales. Para obtener más información, visite es-la.tenable.com.

Configure informes fácilmente

Elabore informes en función de vistas personalizadas (por ejemplo, tipos de vulnerabilidad específicos, vulnerabilidades por host/plug-in, por equipo/cliente) en diversos formatos (HTML, CSV y Nessus XML). Los consultores de seguridad independientes pueden personalizar el título, logotipo y diseño del informe, lo que le permite elaborar informes para diferentes partes interesadas.

Enfoque exacto con las vistas de grupo

Los problemas o las categorías de vulnerabilidades similares se agrupan y se presentan en un solo hilo. La función Posponer les permite a los usuarios la selección de algunos problemas para que desaparezcan de la vista durante un período específico. Esto ayuda a establecer prioridades, lo que le permite centrarse solo en los problemas en los que está trabajando en un momento dado.

Desglose y solución de problemas

A medida que las redes se vuelven más sofisticadas y complejas, concentrarse en los posibles problemas demanda cada vez más tiempo. La funcionalidad de captura de paquetes de Nessus permite una potente capacidad de depuración para solucionar problemas de escaneo.

Evaluación de vulnerabilidades inteligente con Live Results

Live Results realiza una evaluación de vulnerabilidades inteligente en modo fuera de línea con cada actualización de plug-ins, sin tener que ejecutar un escaneo. Simplemente, inicie sesión y vea los resultados de vulnerabilidades potenciales según su historial de escaneos. Con un solo clic, puede ejecutar un escaneo para confirmar la presencia de la vulnerabilidad, lo que crea un proceso más rápido y eficiente para evaluar, priorizar y corregir los problemas.

Portable y flexible

Para mayor portabilidad y facilidad de uso, Nessus está disponible en Raspberry Pi. Esto permite el análisis remoto de Nessus cuando no hay una infraestructura de red que admita la ejecución de Nessus en una computadora portátil. Esto es específicamente útil para los evaluadores de penetración, consultores y otras personas cuya función laboral requiera moverse de una ubicación a otra.

Soporte avanzado disponible

Los clientes de Nessus Expert pueden acceder al correo electrónico, portal, chat y soporte telefónico las 24 horas del día, los 365 días del año, con una suscripción al nivel avanzado de soporte técnico. Esto también ayudará a garantizar tiempos de respuesta y resolución más rápidos. Todos los detalles sobre los planes de soporte se pueden encontrar aquí.