tenable™

Nessus NM™ Manager

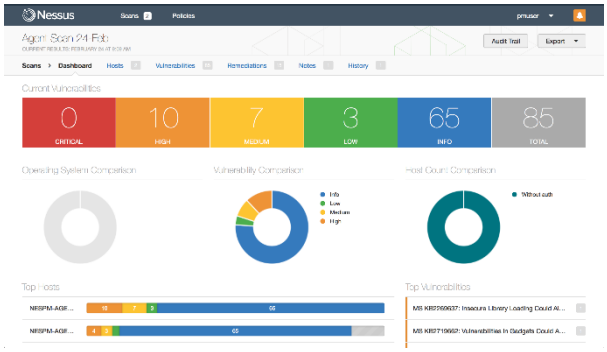
Nessus Manager extiende el poder de Nessus a los equipos de auditoría y seguridad, con escaneo distribuido y gestionado centralmente

Gestión de vulnerabilidad para equipos

Nessus® Manager combina las potentes características de detección, escaneo y auditoría de Nessus, el escáner de vulnerabilidades más implementado en el mundo, con amplias funciones de gestión y colaboración para reducir su superficie de ataque.

Nessus Manager permite el intercambio de recursos, incluidos los escáneres Nessus, programación de escaneos, políticas y resultados de escaneos entre múltiples usuarios o grupos. Los usuarios pueden participar e intercambiar recursos y responsabilidades con sus colegas; responsables de sistemas, auditores internos, personal de cumplimiento y riesgo, administradores de TI, administradores de redes y analistas de seguridad. Estas características colaborativas reducen el tiempo y costo del escaneo de seguridad y auditoría de cumplimiento al simplificar el escaneo, la detección de malware y los errores de configuración, así como también los procesos correctivos.

Nessus Manager protege los entornos físicos, virtuales, móviles y en la nube y y puede implementarse en instalaciones a nivel local. La plataforma de gestión de vulnerabilidad de Tenable.io está disponible para organizaciones que buscan una solución alojada en la nube. Nessus Manager soporta un amplísimo rango de sistemas, dispositivos y activos y, gracias a las dos opciones de implementación –con o sin agente de Nessus–, se amplía fácilmente hacia entornos móviles, transitorios y otros entornos difíciles de alcanzar.



Soporte de varios escáneres

Nessus Manager permite el control de múltiples escáneres Nessus, lo que facilita ampliar la cobertura de escáneres a redes complejas, implementaciones en la nube y ubicaciones distribuidas geográficamente. Los usuarios pueden programar escaneos, impulsar políticas y ver los resultados de escaneos en múltiples escáneres desde una consola central única.

Integración

Nessus Manager se integra con soluciones de gestión de parches de IBM, Microsoft, Red Hat y Dell para ayudar a asegurar que las actualizaciones de software se apliquen a los sistemas y activos, de conformidad con el nivel de criticidad para la organización.

Nessus Manager también se integra con soluciones de gestión de dispositivos móviles (mobile device management, MDM) para Microsoft, Apple, Good, MobileIron y AirWatch para permitir a las organizaciones añadir dispositivos móviles al programa de gestión de vulnerabilidad.

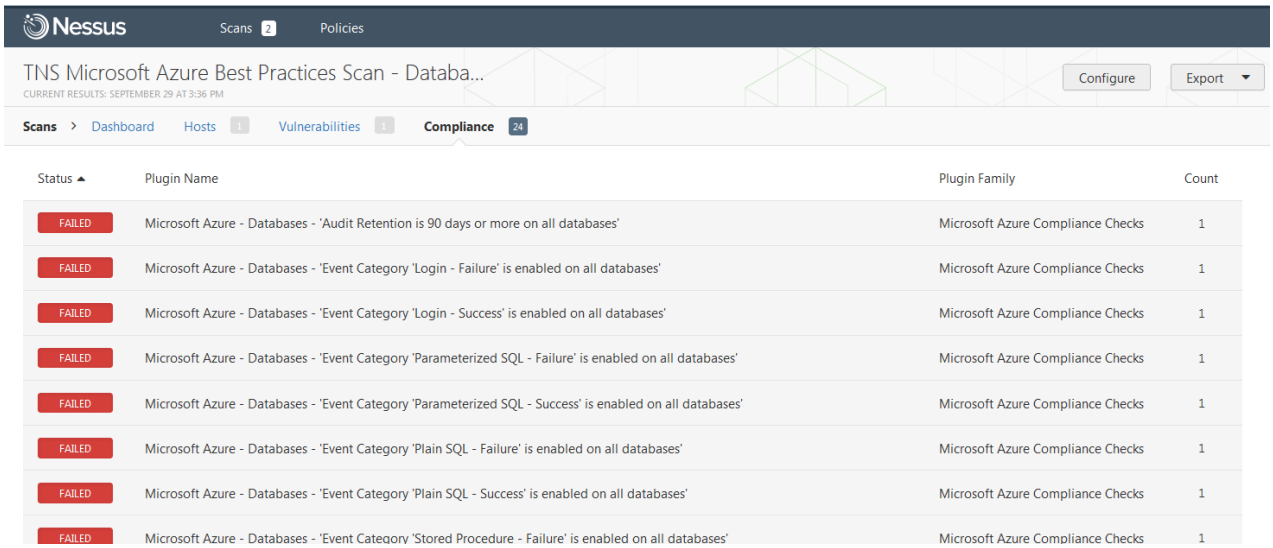
La integración de un almacén de contraseñas con CyberArk facilita la gestión de credenciales para las organizaciones que usan la solución CyberArk.

Nessus Manager reduce la superficie de ataque y ayuda a asegurar el cumplimiento al auditar y escanear implementaciones en la nube tales como Microsoft Azure, AWS y Rackspace.

Beneficios clave

- Escaneo preciso, comprobado y con total soporte: con base en el escáner de vulnerabilidades Nessus
- Intercambio de recursos para mejorar la eficiencia del equipo: permite asignar escáneres, políticas y programaciones e informar el acceso a múltiples usuarios o grupos
- Ampliación de la cobertura de escaneo: permite utilizar los agentes de Nessus para escanear los dispositivos transitorios como laptops o activos donde no tiene las credenciales del servidor
- Mejora del análisis de riesgos: permite incluir contexto a partir de una infraestructura existente y marcos de socios
- Integración con tecnologías centrales: Nessus Manager le permite aprovechar su inversión en tecnologías complementarias como gestión de parches y dispositivos móviles

SC MAGAZINE



Nessus Manager incluye un número de auditorías de configuración para la implementación en la nube, como Microsoft Azure, Amazon Web Services, Rackspace y otras.

Niveles de usuario según función

Nessus Manager permite la adición de múltiples usuarios e introduce cuatro funciones de usuario: administrador del sistema, administrador, estándar y solo lectura. A cada usuario se le pueden asignar diversos niveles de acceso a recursos con base en asociaciones grupales o individuales. Tanto el administrador del sistema como el administrador tienen la autoridad de gestionar usuarios y grupos. Los grupos pueden establecerse según departamentos, funciones de trabajo, tareas o responsabilidades, geografía o lo que mejor responda a sus necesidades específicas.

Equipo de investigación

Las vulnerabilidades y nuevas amenazas son constantes. Por eso, el Equipo de Investigación de Tenable provee actualizaciones frecuentes a Nessus Manager para ayudar a las organizaciones a combatir amenazas avanzadas, vulnerabilidades del "día cero" y nuevos tipos de configuraciones de cumplimiento regulatorio.

La ventaja Nessus

Los clientes eligen a Nessus porque ofrece:

- Escaneo de alta precisión con bajo número de falsos positivos
- Capacidades y características de escaneo integrales
- Escalabilidad a cientos de miles de sistemas
- Implementación y mantenimiento sencillos
- Bajo costo de administración y operación

Agentes de Nessus

Los agentes de Nessus, disponibles con Tenable.io y Nessus Manager, reducen los problemas asociados con el escaneo tradicional de redes, tales como la obtención de credenciales, al tiempo que facilitan el escaneo de una variedad más amplia de activos, incluso fuera de línea.

La mayoría de organizaciones utilizan una mezcla de escaneos con y sin agente en sus entornos Nessus. Los agentes de Nessus podrían ser especialmente atractivos en un número de situaciones, que incluyen:

- **Dispositivos transitorios**: el escaneo de laptops u otros dispositivos transitorios que no siempre están conectados a una red local.
- **Escaneo sin credenciales del servidor**: los activos que se desean o necesitan escanear sin credenciales.
- **Escaneo rápido**: tras la implementación, los agentes utilizan los recursos de servidores locales para escanear y solo utilizan los recursos de la red para enviar resultados de vuelta a Nessus Manager, lo cual facilita las cosas si lo que se desea o requiere es escanear un gran número de activos en poco tiempo.

Capacitación

Tenable ofrece capacitación para quienes no tienen experiencia en el uso de Nessus y desean el conocimiento y capacidades para maximizar el uso del producto, así como temas específicos, como auditorías de cumplimiento para usuarios más avanzados. Los cursos están disponibles a demanda a través del sitio web de Tenable.

tenable™

Para obtener más información: Visite tenable.com

Contáctenos: Escríbanos a subscriptionsales@tenable.com o visite tenable.com/contact