GFI LANguard

Network Security Scanner

Escáner de vulnerabilidad, gestión de parches y auditoría de red

GFI LANguard Network Security Scanner (N.S.S.) es una premiada solución que le permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de su red. Como administrador, usted a menudo tiene que tratar diferentemente problemas relacionados con problemas de seguridad, administración de parches y auditoría de red, a veces utilizando varios productos. Sin embargo, con GFI LANguard N.S.S., esos tres pilares de la administración de vulnerabilidad son abordados en un paquete. Utilizando una única consola con amplias funcionalidades de generación de informes, la solución integrada GFI LANguard N.S.S. le ayuda a abordar estos asuntos más rápida y eficazmente.

GFI LANguard N.S.S. hace uso de avanzadas bases de datos de vulnerabilidades basadas en OVAL y en SANS Top 20, proporcionando más de 15.000 valoraciones de vulnerabilidades cuando su red es escaneada. GFI LANguard N.S.S. le da la información y las herramientas que necesita para realizar escaneos multi plataforma a través de todos los entornos, para analizar el estado de la seguridad de su red y para instalar y administrar eficazmente los parches de todos los equipos a través de diferentes sistemas operativos y en diferentes idiomas. Esto da como resultado un entorno consistentemente configurado que es seguro contra todas las vulnerabilidades.

Votado como el mejor escáner comercial de seguridad de red por los usuarios de Nmap dos años consecutivos, y nombrado ganador en la categoría Gestión de Parches de los premios 'Productos del Año' 2006 de TechTarget, y votado ganador en la categoría de seguridad de los premios Best of TechEd Awards 2007, GFI LANguard N.S.S. es la más completa solución de administración de vulnerabilidades en un paquete convenientemente integrado. GFI LANguard N.S.S. es una solución empresarial esencialy rentable para salvaguardar sus sistemas y redes de ataques hacker y brechas de seguridad.

Beneficios

¿Por qué utilizar GFI LANguard N.S.S.?

- Más de 15.000 estimaciones de vulnerabilidad realizadas a través de su red
- Reduce el coste total de propiedad centralizando el escáner de vulnerabilidad, la gestión de parches y la auditoría de red
- Proporciona informes adaptables de escaneos realizados a través de toda la red incluyendo aplicaciones y recursos
- Ayuda a los administradores de TI a asegurar sus redes más rápido y más eficientemente
- Previene del tiempo de caída y de pérdida de negocio debido a la exposición por vulnerabilidad
- Escáner comercial de seguridad Windows No 1 (votado por los usuarios de NMAP dos años consecutivos) y premio Best of TechEd 2007 (seguridad).

Solución integrada de administración de vulnerabilidades

GFI LANguard Network Security Scanner (N.S.S.) es una premiada solución que dirige los tres pilares de la gestión de vulnerabilidades: análisis de seguridad, administración de parches y auditoría de red mediante una única e integrada consola. Mediante el escaneo de toda la red, identifica todos los posibles problemas de seguridad y utilizando sus extensas funcionalidades de generación de informes le proporciona las herramientas que necesita para detectar, valorar, informar y remediar cualquier amenaza.

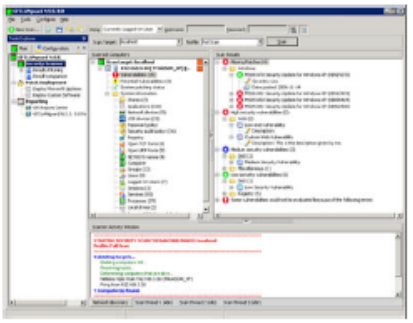
- Análisis de vulnerabilidad
- Administración de parches
- Auditoría de red y de software.

Análisis de vulnerabilidad

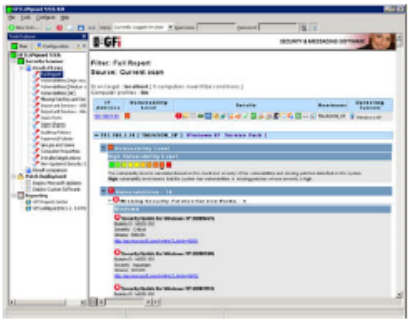
Durante las auditorías de seguridad, se realizan más de 15.000 valoraciones de vulnerabilidad y las redes se escanean IP por IP. GFI LANguard N.S.S. le da la capacidad de realizar análisis multi plataforma ((Windows, Mac OS, Linux) a través de todos los entornos y para analizar el estado de la seguridad de su red desde un único origen de datos. Esto asegura que sea usted capaz de identificar y remediar cualquier amenaza antes de que los hackers lo logren.

GFI LANguard Network Security Scanner

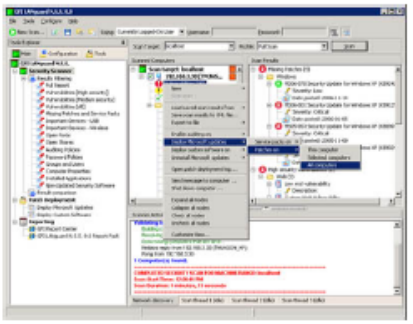
Pantalla principal de GFI LANguard Network Security Scanner



Indica las vulnerabilidades encontradas

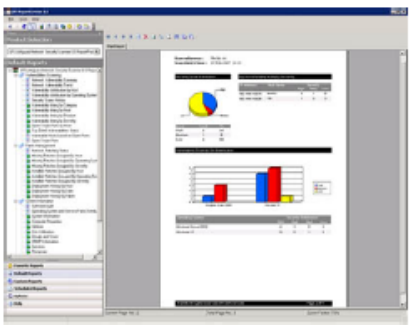


Amplios infomes HTML de seguridad



Implante fácilmente actualizaciones en toda la red

GFI LANguard Network Security Scanner ReportPack



Informe ejecutivo mostrando el resumen de vulnerabilidades de red

Identifica vulnerabilidades de seguridad y toma medidas correctoras

GFI LANguard N.S.S. escanea equipos, identifica y clasifica vulnerabilidades de seguridad, recomienda un curso de acción y proporciona herramientas que le permiten resolver estos asuntos. GFI LANguard N.S.S. también hace uso de un indicador gráfico del nivel de amenaza que proporciona una importante e intuitiva valoración del estado de vulnerabilidad de un equipo o grupo de equipos analizados. Cuando es posible se proporciona un enlace web o más información sobre un asunto de seguridad concreto, como un BugTraq ID o un artículo de la Base de Conocimientos de Microsoft.

Base de datos de vulnerabilidades de gran alcance y potencia industrial

GFI LANguard N.S.S. se entrega con una completa base de datos de valoración de vulnerabilidades, que incluye estándares como OVAL (más de 2.000+ comprobaciones) y SANS Top 20. Esta base de datos se actualiza regularmente con información de BugTraq, SANS Corporation, OVAL, CVE y otras. Mediante su sistema de auto-actualización, GFI LANguard N.S.S. se mantiene siempre actualizado con la información sobre las actualizaciones de seguridad de Microsoft recientemente liberadas así como de las nuevas comprobaciones de vulnerabilidad publicadas por GFI, y otros almacenes de información basados en comunidades tales como la base de datos OVAL.

Asegura que las aplicaciones de seguridad de terceros como anti-virus y anti-spyware ofrecen la protección óptima

GFI LANguard N.S.S. también comprueba que las aplicaciones de seguridad soportadas como anti-virus y anti-spyware están actualizadas con los últimos archivos de definición y que están funcionando correctamente. Por ejemplo, puede asegurar que las aplicaciones de seguridad soportadas tienen habilitadas todas las características clave (como el análisis en tiempo real).

Crea fácilmente diversos tipos de análisis y test de vulnerabilidad

Usted puede fácilmente configurar análisis de diferentes tipos de información; recursos compartidos abiertos en estaciones de trabajo, políticas de seguridad de auditoría/contraseña y equipos que no tienen un parche o service pack concreto. Puede analizar diferentes tipos de vulnerabilidades parta identificar potenciales problemas de seguridad. Estas incluyen:

- **Puertos abiertos:** GFI LANguard N.S.S. escanea puertos innecesariamente abiertos y comprueba que no sea fuercen el hijacking de puertos.
- **Usuarios y grupos locales que no se utilizan:** Eliminar o deshabilitar cuentas de usuario que ya no se usar.
- **Aplicaciones en lista negra:** Identificar software no autorizado o peligroso y agregarlo a listas negras de aplicaciones que usted desee asociar con una alerta de vulnerabilidad de alta seguridad.
- **Dispositivos USB peligrosos, nodos y enlaces inalámbricos:** Busca todos los dispositivos conectados a USB o enlaces inalámbricos y le avisa de cualquier actividad sospechosa.
- ¡Y mucho más!

Cree a medida sus propias evaluaciones de vulnerabilidad

GFI LANguard N.S.S. le permite fácilmente crear a medida evaluaciones de vulnerabilidad mediante un asistente de creación y configuración de una nueva condición de vulnerabilidad. Además puede escribir complejas comprobaciones de vulnerabilidades utilizando el motor de scripts compatible con VBScript de GFI LANguard N.S.S. GFI LANguard N.S.S. incluye un editor y depurador de scripts para ayudar en su desarrollo.

Analice y filtre fácilmente los resultados del análisis

GFI LANguard N.S.S. le permite analizar y filtrar fácilmente los resultados de los análisis haciendo clic sobre uno de los nodos predefinidos del filtro. Esto le permite identificar, por ejemplo, equipos con vulnerabilidades de alta seguridad o equipos a los que les falte un service pack concreto. También se pueden crear muy fácilmente los filtros personalizados desde un principio o los personalizados. También puede exportar los resultados a XML.

Administración de parches

Implante automáticamente parches en toda la red y gestione los service pack

Utilizando GFI LANguard N.S.S. puede implantar fácilmente en toda la red services pack y parches que falten GFI LANguard N.S.S. es la herramienta ideal para monitorizar que Microsoft WSUS esté haciendo su trabajo adecuadamente y realiza las tareas que WSUS no hace como implantar parches de Microsoft Office y de software a medida. GFI LANguard N.S.S. le proporciona también nuevas características como la auto descarga de parches y la retirada de parches. Además cumple con Unicode y es capaz de soportar la gestión de parches en los 38 idiomas actualmente soportados por Microsoft.

Implanta software a medida/de terceros y actualizaciones en toda la red

Además de implantar parches y service packs, GFI LANguard N.S.S. le permite implantar fácilmente software de terceros o actualizaciones en toda la red. Puede utilizar esta característica para implantar software cliente, actualizaciones a medida o software que no es de Microsoft, actualizaciones anti-virus y más. Esta característica de implantación de software a medida significa que usted puede hacerlo sin Microsoft SMS, que es demasiado complejo y caro para redes de tamaño pequeño y mediano.

Auditoría de red y de software

Reciba automáticamente avisos de nuevas brechas de seguridad

GFI LANguard N.S.S. puede realizar análisis programados (por ejemplo, diaria o semanalmente) y puede compararlos automáticamente con resultados de análisis anteriores. Cualquier nueva brecha de seguridad o cambio de configuración descubierto en su red le será enviado por correo para su análisis. Esto le permite identificar rápidamente nuevos recursos compartidos, servicios instalados, aplicaciones instaladas, usuarios agregados, nuevos puertos abiertos y más.

Analice y recupere datos de SO de sistemas Linux

Es posible extraer remotamente datos del SO de sistemas basados en Linux y el resultado se presenta de la misma forma que para equipos basados en Windows. ¡Esto significa que los equipos Linux y Windows se pueden analizar en una sóla sesión de escaneo! GFI LANguard N.S.S. incluye numerosas comprobaciones de seguridad Linux incluyendo detección de rootkit. GFI LANguard N.S.S. puede utilizar archivos de Clave Privada SSH en lugar de las convencionales credenciales de contraseña para autentificarse en equipos Linux.

Requerimientos del sistema

- Sistema operativo Windows 2000 (SP4), XP (SP2), 2003, VISTA
- Internet Explorer 5.1 o superior
- Componente Cliente para Redes Microsoft - incluido por defecto en Windows 95 o superior
- Secure Shell (SSH) - se incluye por defecto en todas las distribuciones del SO Linux.

Premios

Descargue su versión de evaluación de http://www.gfihispana.com/es/lannetscan/

www.cromlec.com

cromlec
...al servei de les persones

Microsoft GOLD CERTIFIED Partner

GFI
www.gfi.com