Auditoría de seguridad sobre configuraciones de equipos de comunicaciones

¿Qué es Rocío?

Rocío es una solución para la automatización de las tareas básicas realizadas por un auditor de seguridad sobre equipos de comunicaciones: enrutadores, conmutadores y cortafuegos. Así, ha sido desarrollada por el CCN-CERT para verificar el nivel de seguridad de dichos equipos. Gracias a ella, los responsables de seguridad podrán comprobar, de un modo rápido y sencillo, si su dispositivo está configurado adecuadamente o no.

¿Por qué usar Rocío?

Su **sistema de autoregistro de usuarios** basado en el correo electrónico permite a los usuarios darse de alta de forma autónoma.

Dentro de cada usuario hay una **sección de proyectos** y de equipos para una mejor organización de los trabajos.

Está desarrollada como una **aplicación web accesible** mediante HTTPS y su soporte de cuenta de usuarios permite que múltiples usuarios la utilicen de manera simultánea.

Se pueden asociar **distintas configuraciones** para cada equipo y se puede tener un conjunto de comandos con distintos apartados.

Propiedades

- Accesible mediante certificado para toda la comunidad del CCN-CERT.
- Se ofrece también como máquina virtual para su uso en entornos aislados, con requisitos de seguridad especiales o sin acceso a Internet.
- Con Rocío se aumenta la frecuencia de la auditoria de redes, ya que se automatiza todo el proceso.
- Permite obtener estadísticas y un histórico de uso con los que realizar búsquedas de párametros de configuración y generar informes de evolución del estado de seguridad de los sistemas.
- Facilita la creación de configuraciones que cumplan la política de seguridad correspondiente.

rocio@ccn-cert.cni.es

¿Cómo funciona?

1º El usuario **carga el fichero de configuración** del equipo a auditar. Adicionalmente, puede cargar también el resultado de la ejecución de algunos comandos que muestren información del sistema. Por ejemplo, tablas de encaminamiento, estado de enlaces o tablas de direcciones, entre otras.

2º El usuario **solicita la realización de la auditoría de seguridad**; que consiste en la comprobación de un conjunto de reglas predefinidas que analizan aspectos de seguridad del equipo, como el cifrado de las contraseñas, la utilización de protocolos de cifrado para el acceso a la gestión o la existencia de listas de acceso.

3º El **resultado de la auditoría** puede verse en pantalla, seleccionando el tipo de regla o su resultado, así como consultar de forma gráfica las líneas de configuración que cada regla ha comprobado. Adicionalmente, el informe de auditoría puede descargarse en forma de documento en formato PDF.