



“Actividad 1”

Guadalupe del Carmen López Sánchez

Licenciatura en Ingeniería En sistemas computacionales y diseño de software,

Instituto Universitario de Yucatán

24040798 :Derecho informático

Ing.Perla Alejandra Landero Heredia

19 de Octubre de 2025

Seguridad Activa

Prevención de amenazas en tiempo real, de los ataques o amenazas en tiempo real con la finalidad de mantener la estabilidad y eficacia de la seguridad.

Seguridad Pasiva

Reduce el impacto del daño a través de un conjunto de medidas reactivas para evitar cualquier ataque.

Vulnerabilidad

Es una debilidad o falta hacia riesgos desconocidos en un sistema.

Herramienta NISUS

Sirve para escaneos gestionados de vulnerabilidades Independientemente del sistema operativo. Encuentra errores de configuración por fallas de actualizaciones o por el propio despliegue. Puede detectar Procesos web y puertos con Sesiones de usuarios mantenidos.

Para configurar un escaneo, se debe añadir una plantilla base que defina los parámetros que escanear una vez configurado dichos parámetros, se le dará un nombre, Juntos a otros datos campos, y se ejecutará de manera automática y periódica o de forma manual.

Funciones NISUS. • Cumplimiento std y normativa asociados a la seguridad Informática • Detección de una alta diversidad de Vulnerabilidades • Fallos en la implementación de configuración std • Gestión de parches en sistemas o periféricos y app que afecten a la seguridad del sistema. • Políticas de Contraseña.

Herramienta NISUS

Sirve para escaneos gestionados de vulnerabilidades Independientemente del sistema operativo. Encuentra errores de configuración por fallas de actualizaciones o por el propio despliegue. Puede detectar Procesos web y puertos con Sesiones de usuarios mantenidos.

Para configurar un escaneo, se debe añadir una plantilla base que defina los parámetros que escanear una vez configurado dichos parámetros, se le dará un nombre, Juntos a otros datos campos, y se ejecutará de manera automática y periódica o de forma manual.

Funciones NISUS. • Cumplimiento std y normativa asociados a la seguridad Informática • Detección de una alta diversidad de Vulnerabilidades • Fallos en la implementación de configuración std • Gestión de parches en sistemas o periféricos y app que afecten a la seguridad del sistema. • Políticas de Contraseña.

NISUS

Es una herramienta de ciberseguridad que realiza el escaneo para identificar Malware y partes traseros y además se utiliza como explorador de puntos débiles.

Malware

Software malicioso con programas o códigos para el robo de datos y es usado por cibercriminales.

Ingresa a www.tenable.com → NISUS → Instalarlo en el botón Try

Mantenimiento.

El buen funcionamiento de Hardware y Software. Consultoría. Hacedores de empresa, esta implementada a mejoras.