Ejercicio X, Seguridad 23-24

Juan Francisco Mier Montoto

**El ejercicio se realiza en la máquina virtual de prácticas y los pasos que se van realizando se documentan con capturas de pantalla, junto a un mínimo texto explicativo:**

## 1. Activar y configurar los controles de seguridad

*Utilizar la herramienta secpol, el Firewall, o incluso propiedades del sistema de ficheros, como la*

*concesión de permisos de acceso. Muchos de los controles que se pueden utilizar ya estarán*

*activados y tendrán una configuración por defecto que aplica el propio sistema.*

*[imágenes aquí]*

## 2. Activar y configurar la auditoría de seguridad, para controlar los eventos que se generan

*El objetivo suele ser recopilar información sobre cuatro aspectos:*

* *Cuando se activa y se desactiva un control, por ejemplo el Firewall.*
* *Cuando se cambia la configuración de un control, por ejemplo las reglas del Firewall.*
* *Cuando el control detecta una violación de seguridad y cual, por ejemplo una denegación de*

*acceso. Esto permite analizar los ataques que han fracasado.*

* *También se puede recabar información de la ausencia de violaciones de seguridad, por*

*ejemplo todos los accesos que permite el Firewall. El volumen de información a tratar*

*aumenta muchísimo. Pero esto permite analizar los ataques que han tenido éxito.*

*La herramienta fundamental para realizar esta tarea es secpol, usando la "Configuración de directiva*

*de auditoría avanzada".*

*[imágenes aquí]*

## 3. Realizar pruebas para generar eventos

*En esta tarea los alumnos deben realizar algunas pruebas para generar eventos de auditoría. Por*

*ejemplo, acceder al sistema dando contraseñas erróneas varias veces y finamente volviendo a*

*entrar con la contraseña correcta. También pueden acceder a archivos cuyo acceso este auditado.*

*Y por supuesto, pueden intentar escanear el computador usando cualquier herramienta de red,*

*como por ejemplo Nmap o Nping.*

*[imágenes aquí]*

## 4. Analizar los registros de eventos de seguridad, para evaluar problemas con la seguridad

*Utilizar el Visor de eventos para analizar los eventos capturados. Se puede vaciar el registro para*

*tener unos pocos eventos y localizarlos rápidamente, pero es más realista no hacerlo. Diseñar algún*

*filtro o alguna consulta para localizar algún tipo de evento en particular y documentarlo. Finalmente,*

*volcar los archivos de eventos para su análisis, utilizando alguna herramienta de análisis de registros*

*o realizando algún tipo de programa que procese eventos.*

*[imágenes aquí]*