**Esquema de ejercicios de auditoría de Windows.**

**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.



En este caso, procederá a activarse esta opción, con lo que podremos auditar cada vez que concedamos permisos de superusuario de manera correcta o errónea.





**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.



En este caso, por cada cambio en el estado de la seguridad, como por ejemplo el Firewall, se lanzará un evento que será recogido por el visor de eventos.

* Cuando se cambia la configuración de un control, por ejemplo las reglas del Firewall.



Permite audiar eventos generados por los cambios en las reglas de directiva que usa el Servicio de Protección de Microsoft, el cual usa el Firewall de Windows.

* Cuando el control detecta una violación de seguridad y cual, por ejemplo una denegación de acceso. Esto permite analizar los ataques que han fracasado.



Permite capturar el acceso a otros objetos, como archivos, ficheros, capertas...

* 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".

**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.



**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 y de modo opcional, volcar los archivos de eventos para su análisis, utilizando alguna herramienta de análisis de registros o realizando algún tipo de programa que procese XML.



Simplemente aplicamos un filtro sencillo, en este caso, que nos muestre todos aquellos errores de auditoría que se han producido en la última hora. Efectivamente, obtenemos dos, que han sido los dos intentos de iniciar sesión de manera incorrecta.

