## 📁 LPIC-2 / 🔒 Examen 212 - Seguridad del Sistema - Ejercicios

*Nota: Estos ejercicios implican instalar software y configurar sistemas de auditoría que pueden generar muchos datos. Realízalos **SIEMPRE en una VM de prueba dedicada**. Asegúrate de que tu VM tiene acceso a internet para la instalación de paquetes. Necesitarás privilegios de superusuario (`sudo`).*

### Ejercicio 12.4.1: Instalando Herramientas de Detección Comunes

- **Objetivo:** Instalar software para FIM y detección de rootkits.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Instala AIDE:** `sudo apt update && sudo apt install aide` (Debian/Ubuntu) o `sudo dnf install aide` (Red Hat/CentOS/Fedora).
    3. **Instala chkrootkit:** `sudo apt install chkrootkit` (Debian/Ubuntu) o `sudo dnf install chkrootkit` (Red Hat/CentOS/Fedora).
    4. **Instala rkhunter:** `sudo apt install rkhunter` (Debian/Ubuntu) o `sudo dnf install rkhunter` (Red Hat/CentOS/Fedora).
    5. **Instala Auditd:** `sudo apt install auditd audispd-plugins` (Debian/Ubuntu) o `sudo dnf install auditd audispd-plugins` (Red Hat/CentOS/Fedora).

### Ejercicio 12.4.2: Inicializando y Ejecutando AIDE

- **Objetivo:** Crear la base de datos inicial de integridad de archivos y ejecutar una verificación.
- **Requisitos:** AIDE instalado. Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Localiza el archivo de configuración de AIDE (Diferencias):** `sudo less /etc/aide/aide.conf` o `sudo less /etc/aide.conf`. Observa las secciones que definen qué directorios se verifican y qué propiedades.
    3. **Inicializa la base de datos de AIDE:** Ejecuta `sudo aide --init`. Esto puede llevar algún tiempo. Creará un archivo como `/var/lib/aide/aide.db.new.gz`.
    4. **Renombra la base de datos para activarla:** Ejecuta `sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz`.
    5. **Ejecuta una verificación de AIDE:** Ejecuta `sudo aide --check`. Dado que no has hecho cambios desde la inicialización (aparte de renombrar el archivo de base de datos, que AIDE puede reportar), la salida debería indicar que no hay cambios significativos o reportar solo el cambio en el propio archivo de base de datos.

6. **Simula un cambio en un archivo no crítico:** Ejecuta `echo "test" | sudo tee /tmp/test_aide.txt`.
7. **Ejecuta otra verificación de AIDE:** `sudo aide --check`. Ahora AIDE debería reportar que `/tmp/test_aide.txt` es un archivo nuevo.
8. **Limpia:** `sudo rm /tmp/test_aide.txt`.
9. **(Conceptual):** Para usar AIDE de forma efectiva, programarías `sudo aide --check` en un cron job y revisarías la salida (que suele enviarse por correo a root o a un log). Después de actualizaciones de software legítimas, necesitarías actualizar la base de datos ejecutando `sudo aide --init` de nuevo y reemplazando el archivo `.db.gz` antiguo.

**Ejercicio 12.4.3: Ejecutando Escaneos de Rootkits (chkrootkit, rkhunter)**

- **Objetivo:** Usar herramientas para buscar rootkits y otras señales de compromiso.
- **Requisitos:** chkrootkit y rkhunter instalados. Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Ejecuta chkrootkit:** Ejecuta `sudo chkrootkit`. Esto ejecutará una serie de pruebas y mostrará el resultado. La salida es a menudo verbosa; busca líneas que indiquen algo "INFECTED" o "VULNERABLE". En una VM limpia, la mayoría de los resultados deberían ser "not found", "nothing", o "no".
    3. **Ejecuta rkhunter (la primera vez puede tardar):** Ejecuta `sudo rkhunter --check`. Te pedirá que presiones Enter varias veces. Ejecuta una serie de pruebas extensas. Busca advertencias (warnings) en la salida. Algunas advertencias pueden ser falsos positivos; investiga las que aparezcan. La primera ejecución crea archivos de propiedades de archivo; las ejecuciones posteriores comparan con estos.
    4. **(Conceptual):** Estos escaneos también deben programarse (cron) y los informes revisarse.

**Ejercicio 12.4.4: Gestión del Servicio Auditd y Archivos de Log**

- **Objetivo:** Asegurarse de que el sistema de auditoría del kernel está funcionando y localizar sus logs.
- **Requisitos:** Auditd instalado. Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Habilita e inicia el servicio:** Ejecuta `sudo systemctl enable auditd && sudo systemctl start auditd`.
    3. **Verifica el estado:** `systemctl status auditd.service`. Debería estar `active (running)`.
    4. **Localiza el archivo de log:** Es `/var/log/audit/audit.log`.

5. **Visualiza el archivo de log (requiere sudo):** Ejecuta `sudo less /var/log/audit/audit.log`. Los mensajes de log de auditd son detallados y pueden ser un poco difíciles de leer sin herramientas como `ausearch`.
6. **Sigue el log en tiempo real:** Ejecuta `sudo tail -f /var/log/audit/audit.log` o `sudo ausearch -i -f`. Mientras se ejecuta, realiza algunas acciones (ej: `ls`, `cd`, `touch /tmp/test.txt`, intenta acceder a un archivo prohibido) y observa los eventos registrados.

**Ejercicio 12.4.5: (Conceptual) Configurando Reglas Básicas de Auditd**

- **Objetivo:** Entender cómo decirle a auditd qué eventos registrar.
- *Requisitos:* Auditd instalado y corriendo. Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Visualiza las reglas actuales cargadas (requiere sudo):** Ejecuta `sudo auditctl -l`. Inicialmente, puede haber reglas por defecto cargadas por archivos en `/etc/audit/rules.d/`.
    3. **Añade una regla temporal para auditar acceso de escritura a un archivo (requiere sudo):** Ejecuta `sudo auditctl -w /etc/passwd -p wa -k passwd_changes`.
        - `-w /etc/passwd`: Vigilar este archivo (watch).
        - `-p wa`: Auditar si se accede con permisos de escritura (`w`) o atributos (`a`).
        - `-k passwd_changes`: Asignar una clave a la regla para facilitar la búsqueda en los logs.
    4. **Intenta modificar el archivo vigilado (requiere sudo):** Ejecuta `sudo vi /etc/passwd` (sin guardar, solo abrir y salir). O `sudo touch /etc/passwd`.
    5. **Verifica los logs de auditd (`/var/log/audit/audit.log`)** (Ej. 12.4.4) o usa `sudo ausearch -k passwd_changes`. Deberías ver eventos registrados relacionados con el acceso de escritura al archivo.
    6. **Las reglas añadidas con `auditctl` se pierden al reiniciar.** Para hacerlas persistentes, añádelas a archivos en `/etc/audit/rules.d/` y recarga el servicio auditd (`sudo systemctl reload auditd` o reinicia).
    7. **(Limpieza en VM):** Elimina la regla temporal si la añadiste: `sudo auditctl -d -w /etc/passwd -p wa -k passwd_changes`. O reinicia la VM.