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

212.4 Intrusion Detection

Teoría

La detección de intrusiones (IDS - Intrusion Detection System) es una parte fundamental de una estrategia de seguridad en profundidad. Su objetivo es detectar intentos de acceso no autorizado o actividades maliciosas y generar alertas para que los administradores puedan responder.

Tipos de IDS:

- **NIDS (Network-based IDS):** Analiza el tráfico de red para identificar patrones de ataque (ej: Snort, Suricata). Se coloca en puntos estratégicos de la red.
- **HIDS (Host-based IDS):** Monitoriza la actividad en un sistema individual (logs del sistema, cambios en archivos, actividad de procesos, llamadas al sistema). Este es el enfoque principal para LPIC-2 212.4.

Componentes y Técnicas Comunes de HIDS en Linux:

1. **Monitorización y Análisis de Logs:**
    - Los archivos de log son la fuente de información más importante. Contienen registros de autenticaciones (exitosas y fallidas), acciones del sistema, errores de servicios, etc.
    - **Logs Relevantes:** `/var/log/auth.log` (Debian/Ubuntu), `/var/log/secure` (Red Hat/CentOS/Fedora) - para autenticación, `journalctl` (si usas systemd), logs específicos de servicios (web server, mail, etc. - Revisado 212.3, 208.2, 211.2).
    - **Herramientas:** `grep`, `awk`, `sed`, scripts personalizados para buscar patrones sospechosos (ej: múltiples intentos de login fallidos desde una IP). Sistemas centralizados de logs (rsyslog, syslog-ng) y herramientas de análisis (SIEM - Security Information and Event Management) son comunes en entornos grandes.
2. **Monitorización de Integridad de Archivos (FIM - File Integrity Monitoring):**
    - Detecta cambios no autorizados (permisos, propietario, hash de contenido, tamaño, etc.) en archivos y directorios críticos del sistema (binarios de comandos, archivos de configuración, archivos de log). Un cambio inesperado puede indicar una intrusión o la instalación de malware.
    - **Herramienta Común: AIDE (Advanced Intrusion Detection Environment)**. Crea una base de datos de la "firma" de los archivos en un estado conocido como "bueno" y luego compara periódicamente el estado actual con esa base de datos.
        - **Configuración:** `/etc/aide/aide.conf` (Debian/Ubuntu) o `/etc/aide.conf` (Red Hat/CentOS/Fedora). Define qué directorios/archivos monitorizar y qué propiedades verificar.

        - **Inicialización de la Base de Datos:** `sudo aide --init`. Crea la base de datos inicial (`/var/lib/aide/aide.db.new.gz` por defecto, que debe renombrarse a `.gz`).
        - **Verificación:** `sudo aide --check`. Compara el estado actual con la base de datos. Reporta los cambios.
    - Las verificaciones de AIDE deben programarse (ej: con cron) y los resultados deben revisarse.
3. **Sistema de Auditoría del Kernel (`auditd`):**
    - Un framework del kernel de Linux que registra eventos de seguridad configurables (llamadas al sistema, acceso a archivos, ejecución de comandos por usuario, cambios de configuración).
    - **Demonio:** `auditd` es el demonio en espacio de usuario que gestiona las reglas y escribe los eventos a los logs.
    - **Configuración de Reglas:** Se define qué eventos auditar. Las reglas pueden añadirse con el comando `auditctl` (temporalmente) o definirse persistentemente en archivos en `/etc/audit/rules.d/` (formato con `-w` para observar archivos/directorios, `-a` para añadir reglas, `-k` para una clave para búsqueda).
    - **Logs:** Los registros de auditoría se guardan en `/var/log/audit/audit.log`. Se pueden consultar y analizar con la herramienta `ausearch` o ver con `less`.
    - `auditd` es muy potente pero puede generar muchos datos; la configuración de reglas es clave.
4. **Detección de Rootkits:**
    - Los rootkits son colecciones de herramientas diseñadas para ocultar la presencia de un atacante en un sistema (ocultar procesos, archivos, conexiones de red).
    - **Herramientas Específicas:**
        - **chkrootkit:** Script que busca signos de rootkits conocidos en archivos del sistema y logs.
        - **rkhunter (Rootkit Hunter):** Herramienta más completa que busca rootkits, backdoors, exploits locales y otras vulnerabilidades, realizando diversas pruebas (hashes de archivos, detección de strings sospechosas, etc.).
    - Deben ejecutarse periódicamente y los resultados revisarse.
5. **Monitorización de Procesos y Uso de Recursos:**
    - Procesos inusuales, uso excesivo de recursos por procesos inesperados, conexiones de red extrañas iniciadas por procesos, pueden ser signos de compromiso.
    - Herramientas como `top`, `htop`, `ps`, `ss`/`netstat` (con `-p`), `lsof`. El sistema de auditoría (`auditd`) también puede configurarse para registrar la ejecución de comandos.
6. **Firewall Logging:** (Revisado 212.2)

- Configurar el firewall para registrar paquetes descartados o rechazados puede ayudar a detectar escaneos de puertos o intentos de conexión a servicios no esperados.

Estrategia de Detección:

Una estrategia de detección de intrusiones efectiva combina varios de estos componentes:

- **FIM (AIDE):** Para detectar cambios no autorizados en el sistema de archivos.
- **Log Management (rsyslog/syslog-ng + análisis):** Para centralizar y analizar logs de diferentes fuentes en busca de patrones.
- **Auditoría (auditd):** Para un registro detallado de eventos de seguridad clave.
- **Rootkit Scanners:** Para buscar malware oculto.
- **Monitorización en Tiempo Real:** Uso de herramientas como `top`, `ss` y revisión de logs en vivo (`tail -f`, `journalctl -f`).

Diferencias Debian vs. Red Hat (IDS):

- Nombres de paquetes para AIDE (`aide`), Auditd (`auditd`), chkrootkit (`chkrootkit`), rkhunter (`rkhunter`) son generalmente estándar.
- La ubicación del archivo de configuración de AIDE puede variar (`/etc/aide/aide.conf` vs `/etc/aide.conf`).
- La ubicación de los archivos de log del sistema (`auth.log` vs `secure`) varía (Revisado 210.2, 212.3).
- La ubicación del directorio de reglas de Auditd (`/etc/audit/rules.d/`) y el archivo de log (`/var/log/audit/audit.log`) son estándar.