Fortalecimiento de Servidores y Redes para Codearts Solutions

---

Fase 1: Análisis inicial del estado del sistema

- Auditoría con lynis para evaluar la seguridad base.
- Revisión de archivos críticos:
  /etc/ssh/sshd_config, /etc/passwd, /etc/shadow, /etc/sudoers
- Verificación de servicios activos con systemctl y puertos con netstat.
- Identificación de configuraciones por defecto o módulos del kernel innecesarios.

Error común:
Lynis no detecta algunas configuraciones por permisos.

Solución:
Ejecutar como root: sudo lynis audit system

Fase 2: Refuerzo de acceso y autenticación

- Desactivar acceso SSH directo como root.
- Obligar uso de claves públicas en SSH.
- Configurar caducidad de contraseñas y bloqueo por intentos fallidos.
- Incluir mensaje legal de advertencia en /etc/issue.net.

Error común:
SSH rechaza conexión tras desactivar el login de root.

Solución:
Asegurarse de tener otro usuario con permisos sudo antes del cambio.

Fase 3: Desactivación de servicios y endurecimiento del kernel

- Detener y deshabilitar servicios no necesarios como CUPS o Avahi.
- Endurecer el kernel con sysctl (IP spoofing, SYN flood, redirects).
- Validar cambios con sysctl -p.

Error común:
No se aplican los cambios de sysctl tras reinicio.

Solución:
Añadir configuraciones persistentes en /etc/sysctl.conf.

Fase 4: Protección de archivos y sistema

- Establecer permisos seguros para archivos sensibles:
    - /etc/shadow → 600
    - /etc/passwd → 644
    - /var/log → root:root, 750
- Activar auditoría con auditd.
- Implementar verificación de integridad con AIDE.

Error común:
AIDE no se inicializa correctamente.

Solución:
Ejecutar aideinit y renombrar la base:
mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Fase 5: Seguridad de red y detección de intrusos

- Aplicar reglas UFW o nftables.
- Configurar fail2ban para protección contra fuerza bruta.
- Instalar psad o portsentry para detectar escaneos y conexiones anómalas.
- Configurar alertas de actividad sospechosa en los logs.

Error común:
Fail2ban no actúa sobre ataques SSH.

Solución:
Revisar logs en /var/log/auth.log y asegurar que coinciden con la configuración de jail.