Investigación Forense de un Incidente en Codearts Solutions

🔹 Fase 1: Identificación y recolección de evidencias

- Se revisaron los principales logs del sistema tanto en Linux (/var/log/auth.log, /var/log/syslog) como en Windows (Event Viewer).
- Se analizó la actividad de usuarios, procesos en ejecución y conexiones de red activas.
- Se realizó un volcado de memoria RAM para preservar evidencias volátiles.

Errores comunes:

- *Olvidar montar volúmenes en solo lectura para evitar alterar evidencia.*
    - Solución: Usar opciones como mount -o ro o herramientas forenses específicas.
- *No registrar la hora del sistema o zona horaria al recopilar logs.*
    - Solución: Documentar el tiempo exacto del sistema antes de iniciar análisis.

🔹 Fase 2: Análisis del incidente y detección del atacante

- Se identificó la IP de origen del ataque mediante revisión de logs y análisis de tráfico.
- Se detectaron archivos modificados y usuarios creados sin autorización.
- Se investigaron comandos sospechosos y posibles backdoors.

Errores comunes:

- *No verificar las tareas programadas (cron, tareas de Windows) como vector de persistencia.*
    - Solución: Revisar crontabs (crontab -l, /etc/crontab) y schtasks en Windows.
- *No validar integridad de binarios del sistema.*
    - Solución: Usar herramientas como debsums, rpm -V o hashes de referencia.

🔹 Fase 3: Extracción y análisis de archivos sospechosos

- Se usaron herramientas como Autopsy, Foremost y Recuva para recuperar datos borrados.
- Se analizaron scripts maliciosos y ejecutables.
- Se revisó el tráfico de red capturado con Wireshark para detectar exfiltración de datos.

Errores comunes:

- *Ejecutar directamente archivos sospechosos sin aislarlos.*
    - Solución: Analizar en máquinas virtuales o entornos de laboratorio.
- *Analizar tráfico sin filtros claros, lo que ralentiza el proceso.*
    - Solución: Aplicar filtros por IP, puerto o protocolo en Wireshark (ip.addr == x.x.x.x).

🔹 Fase 4: Aplicación de medidas de seguridad

- Se desactivaron cuentas comprometidas y se restablecieron contraseñas.
- Se reforzó la configuración del firewall y se implementaron reglas estrictas.
- Se habilitó 2FA para accesos críticos y se configuró un IDS como Snort/Suricata.

Errores comunes:

- *Dejar reglas de firewall por defecto sin validar los nuevos accesos permitidos.*
    - Solución: Revisar todas las reglas activas y aplicar principio de mínimo privilegio.
- *Implementar IDS sin actualizar firmas o configurar alertas.*
    - Solución: Actualizar constantemente y definir notificaciones automáticas por mail/syslog.