Investigación Forense de un Incidente en Codearts Solutions

🔹 Fase 1: Identificación y recolección de evidencias

```
# Revisar logs

less /var/log/auth.log

less /var/log/syslog

journalctl -xe


# Usuarios conectados y procesos

who

last

ps aux


# Conexiones de red

netstat -tulnp

ss -tulnp


# Dump de memoria (ejemplo con LiME o fmem, alternativa básica con dd)

dd if=/dev/mem of=/mnt/usb/mem_dump.raw bs=1M
```

🔹 Fase 2: Análisis del incidente y detección del atacante

```
# Ver IPs sospechosas y actividad

grep 'Accepted' /var/log/auth.log | awk '{print $11}' | sort | uniq -c


# Usuarios sospechosos

cat /etc/passwd | grep '/home'

grep -i 'useradd' /var/log/auth.log


# Buscar comandos ejecutados (historial bash)

cat /home/usuario/.bash_history


# Buscar puertas traseras

find / -type f -perm -4000 2>/dev/null
```

🔹 Fase 3: Extracción y análisis de archivos sospechosos

```
# Recuperación de archivos borrados

foremost -i /dev/sdX1 -o /root/recovered_files/

autopsy # (Interfaz web)

recuva.exe # (Windows)


# Tráfico de red (captura)

tcpdump -i eth0 -w ataque.pcap


# Análisis con Wireshark (GUI o línea)

wireshark ataque.pcap
```

🔹 Fase 4: Aplicación de medidas de seguridad

```
# Desactivar cuentas comprometidas

usermod -L usuario

passwd -l usuario


# Reforzar firewall

ufw enable

ufw default deny incoming

ufw allow ssh


# Implementar 2FA (ejemplo con Google Authenticator)

apt install libpam-google-authenticator

google-authenticator


# Instalar IDS

apt install snort

apt install suricata
```