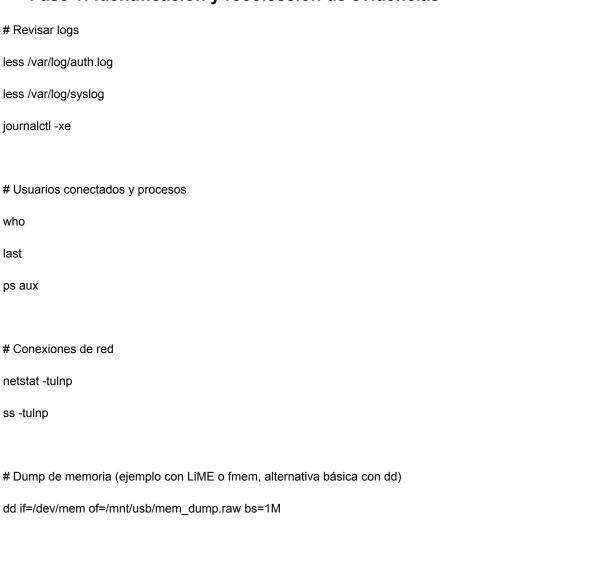
Investigación Forense de un Incidente en Codearts Solutions

Fase 1: Identificación y recolección de evidencias



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

