Detección, Análisis y Eliminación de Malware en Codearts Solutions

---

🔹 Fase 1: Identificación y detección del malware

top

ps aux

netstat -tulnp

ss -tulnp

sudo clamscan -r /

sudo tail -n 100 /var/log/auth.log

sudo tail -n 100 /var/log/syslog

🔹 Fase 2: Análisis del malware y evaluación del impacto

sudo find / -type f -iname "*.enc" -o -iname "*.locked"

sha256sum archivo_sospechoso

strings archivo_sospechoso

hexedit archivo_sospechoso

🔹 Fase 3: Eliminación del malware y recuperación del sistema

sudo kill -9 <PID>

sudo shred -u /ruta/al/archivo_infectado

sudo systemctl restart ssh

sudo tail -n 100 /var/log/syslog

🔹 Fase 4: Implementación de medidas de protección

sudo apt install clamav

sudo freshclam

sudo ufw enable

sudo ufw default deny incoming

sudo ufw allow ssh

sudo apt install libpam-google-authenticator

google-authenticator

sudo iptables -A OUTPUT -p tcp --dport 4444 -j DROP