Práctica 5. Análisis forense de sistemas Linux.

La volatilidad avanzada en Linux. Reto Atenea

Objetivo:

- Aprender a realizar análisis de volcados de memoria en Linux.

Materiales

- Una distribución Linux cualquiera
- Volatility

Una de las alertas del SIEM ha reportado que determinado equipo Linux está realizando multitud de peticiones a una IP externa. Se sospecha que la máquina ha podido ser comprometida. Para comenzar la investigación se ha realizado un volcado de memoria antes de apagar dicho equipo.

Como analista forense deberás identificar el PID dañino responsable de esta alerta (por ejemplo: 1255)

Puede descargar el volcado de memoria aquí.