ÍNDICE

3. Análisis forense en el entorno Linux

3.1 Objetivos

3.2 Visión general del sistema operativo Linux
- 3.2.1 Historia de Linux
- 3.2.2 Las shells de Linux
- 3.2.3 Interfaz gráfica de usuario (GUI)
- 3.2.4 El proceso de arranque (boot) en Linux
- 3.2.5 Gestión de volúmenes lógicos en Linux
- 3.2.6 Distribuciones de Linux

3.3 Técnicas de ocultación
- 3.3.1 Ocultar ficheros y directorios con la shell
- 3.3.2 Ocultar ficheros y directorios con el gestor de ficheros

3.4 Información sobre el sistema y las cuentas
- 3.4.1 Fecha y hora del sistema y versión del sistema operativo
- 3.4.2 Estado actual del sistema
- 3.4.3 Usuarios y contraseñas
- 3.4.4 Configuraciones de usuarios

3.5 Logs y tareas programadas
- 3.5.1 Log /var/log/auth.log
- 3.5.2 Log /var/log/wtmp
- 3.5.3 Log /var/log/btmp
- 3.5.4 Log /var/log/lastlog
- 3.5.5 Log /var/log/kern.log
- 3.5.6 Log /var/log/apport.log
- 3.5.7 Log /var/log/lpr.log
- 3.5.8 Log /var/log/mail.*
- 3.5.9 Log /var/log/mysql.*
- 3.5.10 Log /var/log/apache2/*
- 3.5.11 Tareas programadas

3.6 Información volátil y volcado de memoria
- 3.6.1 AVML: herramienta para realizar el volcado de memoria RAM
- 3.6.2 Volatility en Linux
- 3.6.3 Ejemplos de análisis de memoria con Volatility

3.7 Sistema de ficheros, permisos y directorios de Linux
- 3.7.1 Sistemas de ficheros en Linux
- 3.7.2 Permisos en ficheros y directorios de Linux
- 3.7.3 Marcas de tiempo de ficheros y directorios en Linux
- 3.7.4 Directorios de Linux

3.8 Comandos de shell para análisis forense
- 3.8.1 dmesg
- 3.8.2 fsck
- 3.8.3 grep
- 3.8.4 history
- 3.8.5 mount
- 3.8.6 ps
- 3.8.7 pstree
- 3.8.8 pgrep
- 3.8.9 top
- 3.8.10 kill
- 3.8.11 file
- 3.8.12 su
- 3.8.13 who
- 3.8.14 finger
- 3.8.15 dd
- 3.8.16 ls

3.9 Análisis forense con Kali Linux
- 3.9.1 Kali Linux como entorno de análisis forense
- 3.9.2 Herramientas en Kali Linux para análisis forense