

ÍNDICE

1. Introducción al análisis forense digital

1.1 Objetivos

1.2 Análisis forense digital, metodologías e informes

1.2.1 Definición de análisis forense digital

1.2.2 Metodologías

1.2.3 Estándares en el análisis forense digital

1.2.4 El informe del experto

1.3 Adquisición de evidencias

1.3.1 Manipulación de las evidencias

1.3.2 Medidas para obtención de evidencias

1.3.3 Firma de evidencias y cadena de custodia

1.4 Tipos de almacenamientos y sistema de ficheros

1.4.1 Hardware

1.4.2 Memoria RAM (Random Access Memory)

1.4.3 Discos duros

1.4.4 Software

1.4.5 Ficheros y sistemas de ficheros

1.4.6 Elementos de un disco duro

1.4.7 Extracción de evidencias

1.4.8 Extracción de evidencias por su naturaleza y tecnología

1.5 Metadatos

1.5.1 Qué son los metadatos

1.5.2 Tipos de metadatos

1.5.3 Uso de los metadatos

1.5.4 Ejemplos de metadatos

1.5.5 Los metadatos como prueba

1.6 Redes y direcciones

1.7 Redes de ordenadores

1.7.1 Direcciones

1.8 Herramientas software para el análisis forense

1.8.1 Autopsy

1.8.2 Kali Linux

1.8.3 CAINE

1.8.4 EnCase

1.8.5 FTK

1.8.6 Digital Forensics Framework

1.8.7 Volatility

1.8.8 Redline

1.8.9 COFEE

1.8.10 Wireshark

1.8.11 DumpZilla

1.8.12 Estación de trabajo SIFT

1.8.13 Exiftool

1.8.14 Bulk Extractor

1.9 Técnicas anti-forenses

1.9.1 Definición de técnicas anti-forenses

1.9.2 Borrado de ficheros

- 1.9.3 Protección mediante contraseñas
- 1.9.4 Cifrado de discos
- 1.9.5 Protocolos de red que cifran la información
- 1.9.6 Esteganografía
- 1.10 Conclusiones
- 1.11 Bibliografía
- 1.12 Test de conocimientos básicos
- 1.13 Ejercicios resueltos
- 1.14 Proyecto práctico
 - 1.14.1 Título y enunciado
 - 1.14.2 Solución

2. Análisis forense en el entorno Windows

- 2.1 Objetivos
- 2.2 Visión general del sistema operativo Windows
 - 2.2.1 Historia de Windows
 - 2.2.2 Procesamiento con 64 bits
 - 2.2.3 El proceso de arranque (boot)
 - 2.2.4 Ficheros importantes
- 2.3 Información volátil y adquisición de memoria
 - 2.3.1 Memoria volátil
 - 2.3.2 Identificación de información volátil
 - 2.3.3 Adquisición de memoria RAM
- 2.4 Análisis de la memoria RAM
 - 2.4.1 Hora del sistema
 - 2.4.2 Usuarios logueados
 - 2.4.3 Conexiones y estado de la red
 - 2.4.4 Ficheros abiertos
 - 2.4.5 Información de procesos
 - 2.4.6 Contenido del portapapeles (clipboard)
 - 2.4.7 Historial de comandos
 - 2.4.8 Análisis de memoria con FTK Imager y Volatility
- 2.5 Información no volátil: swap, shadow y logs
 - 2.5.1 Fichero swap de Windows
 - 2.5.2 Copia de seguridad shadow
 - 2.5.3 Logs de Windows
- 2.6 Directorios y ficheros de Windows
 - 2.6.1 Directorios de Windows
 - 2.6.2 Espacio no asignado
 - 2.6.3 Historial de navegación eliminado
 - 2.6.4 Ficheros y permisos en Windows
- 2.7 Registro de Windows
 - 2.7.1 Definición del registro de Windows
 - 2.7.2 Componentes del registro
- 2.8 Papelera de reciclaje y PowerShell
 - 2.8.1 Papelera de reciclaje
 - 2.8.2 PowerShell
- 2.9 Conclusiones
- 2.10 Bibliografía
- 2.11 Test de conocimientos básicos
- 2.12 Ejercicios resueltos
- 2.13 Proyecto práctico
 - 2.13.1 Título y enunciado
 - 2.13.2 Solución

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/appport.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

- 3.10 Conclusiones
- 3.11 Bibliografía
- 3.12 Test de conocimientos básicos
- 3.13 Ejercicios resueltos
- 3.14 Proyecto práctico
 - 3.14.1 Título y enunciado
 - 3.14.2 Solución

4. Análisis de redes y tráfico

- 4.1 Objetivos
- 4.2 Conceptos generales de redes de comunicaciones
 - 4.2.1 Modelos de red OSI y TCP/IP
 - 4.2.2 Direcciones MAC
 - 4.2.3 Direcciones IP
 - 4.2.4 Protocolos de transporte y puertos en TCP y UDP
 - 4.2.5 Aplicaciones
 - 4.2.6 Firewall, IDS, IPS y SIEM: conceptos básicos
- 4.3 Herramientas para el análisis de tráfico
 - 4.3.1 Wireshark
 - 4.3.2 Nmap
 - 4.3.3 tcpdump
 - 4.3.4 NetworkMiner
 - 4.3.5 Snort
- 4.4 Análisis de paquetes, tráfico y logs
 - 4.4.1 Captura de tráfico en redes cableadas
 - 4.4.2 Captura de tráfico inalámbrico
 - 4.4.3 Captura y análisis de paquetes con Wireshark
 - 4.4.4 Captura y análisis de tráfico con NetworkMiner
 - 4.4.5 Logs de red
- 4.5 Análisis forense en proxies
 - 4.5.1 Concepto de proxy
 - 4.5.2 Tipos de proxies
 - 4.5.3 Análisis con el proxy Squid
- 4.6 Análisis forense en firewalls
 - 4.6.1 Concepto de firewall
 - 4.6.2 Tipos de firewalls
 - 4.6.3 Análisis de logs en firewalls
- 4.7 Análisis forense en routers
 - 4.7.1 Concepto de router
 - 4.7.2 Información disponible en los routers
- 4.8 Conclusiones
- 4.9 Bibliografía
- 4.10 Test de conocimientos básicos
- 4.11 Ejercicios resueltos
- 4.12 Proyecto práctico
 - 4.12.1 Título y enunciado
 - 4.12.2 Solución

5. Análisis del malware

- 5.1 Objetivos
- 5.2 Concepto y tipos de malware
 - 5.2.1 Definición de malware
 - 5.2.2 Objetivos del malware
 - 5.2.3 Origen y evolución del malware
 - 5.2.4 Tipos de malware

- 5.3 Impactos del malware
 - 5.3.1 Misión del malware
 - 5.3.2 Malware destructivo
 - 5.3.3 Robo de identidad
 - 5.3.4 Espionaje
 - 5.3.5 Fraude financiero
 - 5.3.6 Robo de datos
 - 5.3.7 Uso indebido de recursos
- 5.4 Ciclo de vida de un ciberataque
 - 5.4.1 Etapas de un ciberataque
 - 5.4.2 Reconocimiento
 - 5.4.3 Armatización
 - 5.4.4 Entrega
 - 5.4.5 Explotación
 - 5.4.6 Instalación
 - 5.4.7 Mando y control
 - 5.4.8 Acción sobre los objetivos
 - 5.4.9 Métodos para detener los ataques
- 5.5 Indicadores de compromiso (IOC)
 - 5.5.1 Definición de indicadores de compromiso (IOC)
 - 5.5.2 IOC vs. IOA
 - 5.5.3 Tipos de indicadores de compromiso
 - 5.5.4 Ejemplos de IOC
 - 5.5.5 Mejores prácticas en la gestión de IOC
- 5.6 Tipos de análisis de malware
 - 5.6.1 Objetivos del análisis de malware
 - 5.6.2 Tipos de análisis de malware
 - 5.6.3 Casos de uso en el análisis de malware
- 5.7 Análisis estático
 - 5.7.1 Técnicas de análisis estático
 - 5.7.2 Determinar el tipo de fichero
 - 5.7.3 Huellas dactilares (hash) del malware
 - 5.7.4 Escaneado antivirus múltiple
 - 5.7.5 Extracción de cadenas de caracteres
 - 5.7.6 Ofuscación de ficheros
 - 5.7.7 Comparación y clasificación del malware
- 5.8 Análisis dinámico
 - 5.8.1 Fases del análisis dinámico
 - 5.8.2 Supervisión de sistemas y redes
 - 5.8.3 Herramientas para análisis dinámico
 - 5.8.4 Inspección de procesos con System Informer
 - 5.8.5 Interacción con el sistema con Process Monitor
 - 5.8.6 Registro de actividad del sistema con Noriben
 - 5.8.7 Captura de tráfico de red con Wireshark
 - 5.8.8 Simulación de servicios con INetSim
- 5.9 Conclusiones
- 5.10 Bibliografía
- 5.11 Test de conocimientos básicos
- 5.12 Ejercicios resueltos
- 5.13 Proyecto práctico
 - 5.13.1 Título y enunciado
 - 5.13.2 Solución

6. Análisis del correo electrónico

- 6.1 Objetivos
- 6.2 Descripción del servicio de correo electrónico
 - 6.2.1 Servicio de correo electrónico

- 6.2.2 Infraestructura del servicio de correo electrónico
- 6.2.3 Agentes de correo
- 6.2.4 Servidores de correo
- 6.2.5 Direcciones IP
- 6.2.6 Dominios de envío
- 6.2.7 Protocolos de autenticación
- 6.2.8 Bucles de realimentación
- 6.3 Protocolos: SMTP, IMAP, POP3 y HTTP/S
 - 6.3.1 Qué es un protocolo de correo electrónico
 - 6.3.2 SMTP: Simple Mail Transfer Protocol
 - 6.3.3 IMAP: Internet Message Access Protocol
 - 6.3.4 POP3: Post Office Protocol
 - 6.3.5 Comparativa entre IMAP y POP3
 - 6.3.6 Puertos utilizados en el servicio de correo electrónico
 - 6.3.7 Protocolo HTTP/HTTPS para webmail
 - 6.3.8 Envío y recepción de un correo electrónico
- 6.4 Descifrado del correo electrónico
 - 6.4.1 Decodificación de un email
 - 6.4.2 Cabeceras
 - 6.4.3 Cómo ver las cabeceras de los correos electrónicos
 - 6.4.4 Cabeceras informativas
 - 6.4.5 Cabeceras técnicas
 - 6.4.6 Cabeceras de seguridad
 - 6.4.7 Cabeceras X-headers
- 6.5 Análisis de clientes de correo y webmails
 - 6.5.1 Análisis del correo electrónico basado en cliente
 - 6.5.2 Microsoft Outlook y Outlook Express
 - 6.5.3 Microsoft Windows Live Mail
 - 6.5.4 Mozilla Thunderbird
 - 6.5.5 Análisis de webmail
- 6.6 Herramientas para el análisis de correo electrónico
 - 6.6.1 Herramientas para el análisis de cabeceras
 - 6.6.2 Messageheader Toolbox
 - 6.6.3 Mx Toolbox
 - 6.6.4 Mailheader
 - 6.6.5 Análisis forense en servidores de correo
- 6.7 Conclusiones
- 6.8 Bibliografía
- 6.9 Test de conocimientos básicos
- 6.10 Ejercicios resueltos
- 6.11 Proyecto práctico
 - 6.11.1 Título y enunciado
 - 6.11.2 Solución

A. Soluciones de los tests de conocimientos básicos

B. Soluciones de los ejercicios

Índice de figuras

Índice de tablas

Bibliografía