EXAMEN SIMULACRO - ANÁLISIS FORENSE INFORMÁTICO

# PREGUNTAS GENERALES (24 preguntas tipo test)

Seleccione la única respuesta correcta para cada pregunta.

1. ¿Cuál es el objetivo principal del análisis forense informático?

* ✔ A) Extraer datos para resolver un delito
* B) Optimizar el rendimiento del equipo
* C) Actualizar el sistema operativo
* D) Eliminar malware del sistema

2. ¿Qué tipo de datos se consideran volátiles?

* A) Configuraciones del sistema
* B) Archivos del sistema
* ✔ C) Memoria RAM
* D) Registros de logs

3. ¿Qué técnica se emplea para evitar la contaminación de evidencias?

* A) Modificar las evidencias en el sistema
* ✔ B) Trabajar con copias de los soportes
* C) Utilizar herramientas no certificadas
* D) Analizar directamente el disco original

4. ¿Qué herramienta se utiliza para la adquisición de memoria RAM en Windows?

* A) Wireshark
* B) Volatility
* C) Autopsy
* ✔ D) Memoryze

5. ¿Qué comando de Windows permite ver las conexiones de red activas?

* A) ipconfig
* B) ping
* C) tracert
* ✔ D) netstat

6. ¿Qué tipo de análisis se recomienda en sistemas críticos en funcionamiento?

* A) Análisis post mortem
* ✔ B) Análisis en caliente
* C) Análisis en frío
* D) Análisis de red

7. ¿Qué herramienta permite clonar discos duros para el análisis forense?

* ✔ A) FTK Imager
* B) Volatility
* C) Memoryze
* D) Wireshark

8. ¿Qué herramienta permite adquirir memoria RAM en sistemas Linux?

* A) Wireshark
* B) Volatility
* C) Memoryze
* ✔ D) LiME

9. ¿Qué técnica se usa para garantizar la persistencia en Linux?

* A) Uso de Memoryze en RAM
* B) Utilización de Wireshark
* C) Análisis de logs con FTK Imager
* ✔ D) Configuración de tareas en crontab

10. ¿Cuál es la principal función de Volatility en el análisis forense?

* A) Análisis de discos duros
* B) Análisis de redes
* C) Análisis de aplicaciones
* ✔ D) Análisis de memoria RAM

11. ¿Qué plugin de Volatility se usa para identificar procesos ocultos?

* A) connections
* B) pslist
* ✔ C) psscan
* D) pstree

12. ¿Qué comando permite ver las conexiones activas con Volatility?

* A) pstree
* ✔ B) connections
* C) pslist
* D) hivelist

13. ¿Qué herramienta se usa para analizar el registro de Windows en Volatility?

* ✔ A) hivelist
* B) psxview
* C) connscan
* D) sockscan

14. ¿Qué técnica antiforense puede usar un malware para evitar ser detectado?

* A) Modificar archivos del sistema
* B) Generar logs falsos
* C) Eliminar procesos legítimos
* ✔ D) Descargarse de la memoria al detectar depuración

15. ¿Qué modelo de servicio en la nube proporciona infraestructura hardware y redes?

* A) DaaS
* ✔ B) IaaS
* C) SaaS
* D) PaaS

16. ¿Qué técnica mejora la seguridad física de un centro de datos en la nube?

* A) Desactivar logs
* B) Uso de puertos no estándar
* ✔ C) Redundancia de hardware
* D) Permitir acceso sin autenticación

17. ¿Qué herramienta es específica para el análisis forense en entornos cloud?

* ✔ A) Cellebrite UFED Cloud Analyzer
* B) Volatility
* C) ProcMon
* D) Wireshark

18. ¿Qué modelo de servicio cloud permite mayor control en el análisis forense?

* A) FaaS
* B) PaaS
* C) SaaS
* ✔ D) IaaS

19. ¿Qué dominio del análisis forense en cloud aborda el cumplimiento legal?

* ✔ A) Dominio regulatorio
* B) Dominio técnico
* C) Dominio organizativo
* D) Dominio operacional

20. ¿Qué malware es conocido por comprometer dispositivos IoT?

* A) Stuxnet
* B) Petya
* C) Wannacry
* ✔ D) Mirai

21. ¿Qué técnica forense se usa en drones para extraer evidencias?

* A) Desmontar el dispositivo
* B) Análisis de red
* ✔ C) Conexión USB a la memoria interna
* D) Acceso remoto

22. ¿Qué recomendación mejora la seguridad de los dispositivos IoT?

* A) Desactivar el cifrado TLS
* B) Permitir accesos remotos sin restricciones
* ✔ C) Usar segmentación de red
* D) Usar credenciales por defecto

23. ¿Qué norma establece directrices para la redacción de informes forenses?

* ✔ A) UNE 197010:2015
* B) ISO 27001
* C) CIS Controls
* D) NIST 800-53

24. ¿Qué herramienta permite visualizar logs centralizados en la plataforma ELK?

* A) Logstash
* ✔ B) Kibana
* C) Elasticsearch
* D) Splunk

# CASO PRÁCTICO (6 preguntas tipo test)

Una empresa tecnológica ha detectado actividad sospechosa en uno de sus servidores críticos: hay múltiples conexiones de red no autorizadas, el sistema muestra procesos activos anómalos, y varios empleados han accedido desde sus dispositivos móviles sin las medidas de seguridad requeridas. El equipo de ciberseguridad inicia una investigación forense completa. Se analiza la memoria RAM, el tráfico de red, y se requiere la adquisición de evidencias tanto del servidor como de terminales móviles.

25. ¿Qué herramienta debería utilizar el equipo para analizar los procesos activos en la memoria del servidor?

* A) FTK Imager
* B) Autopsy
* ✔ C) Volatility
* D) ADB

26. ¿Qué plugin de Volatility es adecuado para identificar DLLs inyectadas por malware?

* A) pslist
* B) hivelist
* C) psscan
* ✔ D) malfind

27. ¿Qué técnica se recomienda aplicar al disco afectado para evitar la alteración de evidencias?

* A) Analizar el disco directamente
* B) Realizar un análisis post mortem
* C) Utilizar herramientas de sniffing
* ✔ D) Clonar el disco y trabajar sobre la copia

28. En caso de que se detecte acceso mediante un dispositivo Android, ¿qué herramienta puede ser útil para investigar el terminal?

* A) Cellebrite Touch
* ✔ B) ADB
* C) Volatility
* D) Wireshark

29. Si se quiere verificar conexiones de red activas durante el incidente, ¿qué herramienta puede mostrar esa información en tiempo real?

* A) ProcMon
* B) Autopsy
* ✔ C) Wireshark
* D) Recuva

30. ¿Qué medida preventiva ayudaría a evitar accesos no autorizados desde dispositivos móviles?

* A) Permitir conexiones remotas sin cifrado
* B) Usar contraseñas por defecto
* ✔ C) Implementar autenticación multifactor
* D) Compartir credenciales por correo