Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA TEÓRICA FINAL MF0488_3 : Gestión de Incidentes de Seguridad Informática			Fecha	07 / 08 / 2019
			Página 1 de 21	
Curso	SEGURIDAD INFORMATICA	**Código del curso**	18-38/000057	

Nombre y Apellidos:			
DNI:		**Firma del Alumno:**	
DOCENTE:	Fabián Rosquete Hernández	**Firma del Docente:**	

Apto: ☐ **No Apto:** ☐ **Calificación:** ☐

INSTRUCCIONES GENERALES:

Lee detenidamente las preguntas y contesta, **con bolígrafo azul**. Al finalizar la prueba y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

La prueba tiene un total de 50 items con un valor de 1 punto cada uno, distribuidos de la siguiente forma :

- **ÍTEMS DE SELECCIÓN MULTIPLE (25 Items) = 25 puntos**

  Para contestar a los ítems de selección simple, rodea con un círculo la opción adecuada. Si te equivocas pones una cruz al lado y rodeas con el círculo la opción correcta.

  (Fórmula de corrección : **Puntuación = Aciertos – (Errores / 3)**)

- **ÍTEMS DE VERDADERO/ FALSO (10 items) = 10 puntos**

  Para contestar a los ítems de Verdadero o Falso, en el recuadro de cada pregunta pon :

  - "**V**" si consideras que es verdadera
  - "**F**" si consideras que es falsa

  Si te equivocas, táchala pon la respuesta que consideres correcta.

  (Fórmula de corrección : **Puntuación = Aciertos – Errores**)

- **ÍTEMS DE TEXTO INCOMPLETO (6 items) =6 puntos**

  (Fórmula de corrección : **Puntuación = Aciertos**)

PRUEBA OBJETIVA TEÓRICA FINAL MF0488_3 : Gestión de Incidentes de Seguridad Informática			Fecha	07 / 08 / 2019
			Página 2 de 21	
Curso	SEGURIDAD INFORMATICA	**Código del curso**	18-38/000057	

INSTRUCCIONES GENERALES:

- **ÍTEMS DE CORRESPONDENCIA (6 Items) = 6 puntos**

  Para contestar a los ítems de correspondencia, hay que identificar cada elemento de la columna de la izquierda con su correspondiente elemento de la columna de la derecha.

  Cada correspondencia establecida correctamente tendrá la siguiente puntuación según el número de errores cometidos en el conjunto de ítems de correspondencia:

ERRORES	PUNTOS
0	1
1	0,8
2	0,6
+3	0

  (Fórmula de corrección : **Puntuación = Aciertos**)

- **ÍTEMS DE ENSAYO BREVE (3 Items) = 3 puntos**

  Para contestar a los ítems de ensayo breve, hay que sintetizar la respuesta en a lo sumo tres frases.

  (Fórmula de corrección : **Puntuación = Aciertos**

Dispones de 1 hora para realizar la prueba.

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA TEÓRICA FINAL MF0488_3 : Gestión de Incidentes de Seguridad Informática			Fecha	07 / 08 / 2019
Curso	SEGURIDAD INFORMATICA	**Código del curso**	18-38/000057	

BLOQUE DE ITEMS DE SELECCIÓN MULTIPLE

Para contestar a los ítems de selección múltiple, rodea con un círculo la opción adecuada. Si te equivocas pones una cruz al lado y rodeas con el círculo la opción correcta.

Cada ITEM tiene un valor de 1 punto

Fórmula de corrección : **Puntuación = Aciertos – (Errores / 3)**

Calificación

1	2	3	4	5	6	7	8	9	10	11	12

13	14	15	16	17	18	19	20	21	22	23	24	25

1. Indique cuál de las siguientes opciones no se corresponde con los beneficios que aporta una correcta gestión de incidentes en las organizaciones.

a. Rápida restauración del sistema informático garantizando la mínima pérdida de información posible.
b. Mejora continua de la gestión y tratamiento de incidentes.
c. Menor control de los procesos del sistema de información.
d. Optimización de los recursos disponibles.

2. Indique cuál de las siguientes oraciones no se corresponde con las ventajas de los sistemas de detección de intrusos basados en red o NIDS.

a. Son sistemas de fácil instalación y actualización.
b. Detectan accesos no deseados en la red.
c. Pueden operar y detectar ataques ante datos cifrados que circulan por la red.
d. Tienen un bajo impacto en la red al no intervenir en sus operaciones habituales.

3. Indique cuál de las siguientes opciones caracteriza la zona roja en la seguridad perimetral.

a. Esta zona el IDS/IPS tiene que configurarse de modo que tenga mayor sensibilidad.
b. En esta zona cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como hostil.
c. En esta zona el sistema IDS/IPS debe configurarse de modo que tenga poca sensibilidad ya que observará todo el tráfico de la red y habrá una elevada posibilidad de falsas alarmas. pag39

4. Indique cuál de las siguientes oraciones no es un tipo de incidente de Acceso no autorizado.

a. Accesos no autorizados con éxito.
b. Alteración de la información.
c. Abuso o mal uso del correo electrónico.
d. Borrado de la información.

5. Indique cuál de las siguientes frases no forma parte del funcionamiento de un IDS

a. Bases de datos
b. Configuración
c. Detección
d. Bloqueo y eliminación 22

6. Indique cuál de las siguientes ventajas no está ofrecida por el IDS/IPS situado detrás del cortafuegos.

a. El riesgo de ataques exitosos disminuye considerablemente.
b. Al poder identificar los ataques más comunes permite una configuración más efectiva del cortafuegos principal.
c. Permite una correlación entre los ataques detectados antes y después del cortafuegos.57
d. La cantidad de logs es inferior, pero la información facilitada por estos sistemas está mejor seleccionada y es más relevante.

7. ¿Cuál de los siguientes aspectos no se incluye en el análisis previo para implantar un sistema IDS/IPS en una organización?

a. Análisis de los protocolos de red utilizados.
b. Análisis de las zonas externas de la organización.62
c. Análisis de los servicios que ofrece la organización.
d. Análisis de los procesos de negocio e identificación de la información valiosa en cada uno de los procesos.

8. Indique cuál de los siguientes datos no está contenido en un evento en el registro de auditoría.

a. La acción realizada.
b. El éxito o fracaso del evento.
c. La funcionalidad del evento.82
d. El usuario que ha realizado la acción.

9. Indique cuál de los siguientes análisis de los datos obtenidos por los IDS/IPS no es un tipo de análisis.

a. Detección de usos indebidos por lotes en tiempo real
b. Detección de anomalías
c. Análisis por lotes
d. Análisis a tiempo real

10. Indique cual de las pruebas de configuración de un IDS/IPS citadas a continuación no hay que tener en cuenta como una de las causas más frecuentes de falsos positivos

a. Actividad del sistema de supervisión de red
b. Escaneo de vulnerabilidad y escáneres de puertos de red
c. Cadenas cortas de registro web 72
d. Comportamientos similares a troyanos o gusanos

11. Indique cuál de los siguientes aspectos no es común a los distintos tipos de códigos maliciosos.

a. Es habitual que se instalen con el consentimiento del usuario.
b. Para lograr sus objetivos necesitan un sistema de cómputo anfitrión.
c. En su funcionamiento interfieren con la operación normal del sistema al que atacan.
d. Suelen ser componentes de software diseñados con un fin específico.

12. De las siguientes opciones indique cuál de ellas no se corresponde con información que facilita la herramienta Virus total.

a. Información detallada del archivo analizado.
b. Comentarios de los intrusos sobre el archivo.
c. Votos positivos o negativos de los usuarios sobre el archivo.
d. Resultado positivo o negativo del análisis realizado por los distintos motores de antivirus y anti-malware.

13. Indique cuál de los siguientes conceptos no se corresponde con una vía de acceso de código malicioso al equipo.

a. Navegadores.
b. Red local.
c. Antivirus.
d. Correo electrónico.

14. Cual de las siguientes frases no caracteriza al Wireshark.

a. Captura los paquetes directamente desde una interfaz de red.
b. Permite obtener información detallada del protocolo utilizado en el paquete de datos capturado.
c. Puede importar y/o exportar los registros capturados desde/hacia otras aplicaciones.
d. No busca los registros de información que cumplan con un criterio establecido previamente por el usuario.133

15. Cual no es uno de los objetivos del software tipo código maliciosos o malware.

a. Destruir datos, eliminando archivos o, incluso, formateando discos.
b. Robar información y claves.
c. Comprometer sistemas operativos.
d. busca los registros de información que cumplan con un criterio establecido previamente por el usuario.99

16. Indique cuál de las siguientes funciones no se corresponde con los sistemas de información y eventos de seguridad o SIEM.

a. Conocimiento del comportamiento del usuario y su contexto.
b. Incumplimiento de nuevas normativas de seguridad.170
c. Detección de anomalías y amenazas.
d. Administración más efectiva del riesgo.

17. Indique cual de las siguientes funcionalidades no es válida para un sistema de gestión de seguridad de la información o SIM.

a. Predecir y pronosticar amenazas.
b. Centralizar y monitorizar los componentes de la infraestructura de la organización.
c. Seguimiento de los incidentes de seguridad a tiempo real.168
d. Realizar un análisis forense de los eventos de seguridad.

18. Indique cual de las siguientes actividades no contiene el informe que hay que realizar en la investigación de un incidente

a. Análisis de las consecuencias que hayan podido afectar a terceros.
b. Análisis de la información del incidente compartida con terceros.
c. Revisión exhaustiva de los logs de los equipos, sistemas y dispositivos afectados por el incidente.
d. Seguimiento de los incidentes de seguridad a tiempo real.174

19. Indique cuál de los siguientes aspectos no se considera necesario que esté contenido en el registro de gestión de incidencias.

a. El tipo de incidencia.
b. La persona que realiza la notificación.
c. Los efectos que no han derivado de la misma.200
d. El momento en el que se produce la incidencia.

20. Indique cuál de los siguiente conceptos no se debe contener en la estructura de un plan de recuperación de desastres:

a. Análisis de impacto al negocio.
b. Plan de trabajo con la planificación de las intrusiones de la organización.245
c. Definición de los requisitos de la organización en cuanto a las necesidades de recuperación, el ámbito de aplicación y sus objetivos.
d. Informes de la evaluación de la seguridad y la vulnerabilidad de los sistemas.

21. Indique cuál de los siguiente conceptos no es una topología para detectar el tráfico de red malicioso de los IPS

a. Detección basada en firmas
b. Detección basada en registros de la CPU217
c. Detección basada en anomalías
d. Detección *honey pot* o jarra de miel

22. Indique cuál de las siguientes frases no es una fase del análisis informático forense:

a. Contención, erradicación y recuperación de datos
b. Adquisición de datos y recopilación de evidencias
c. Análisis e investigación de las evidencias
d. Confirmación de las pruebas realizadas y realización del informe

23. Indique cuál de los siguientes objetivos no corresponde a la informática forense:

a. Compensar los daños causados por los intrusos.
b. Aplicar medidas preventivas a los atacantes.
c. Crear e implantar medidas para prevenir incidentes futuros similares.
d. Perseguir y aplicar medidas judiciales a los atacantes.

24. Indique cuál de los siguientes requisitos no se corresponde con los necesarios para que una evidencia pueda ser admitida como tal.

a. La evidencia debe conservarse en un estado lo más parecido al estado en el que se encontró.
b. Las evidencias digitales deberán documentarse con firmas digitales del investigador para garantizar que nadie más realiza ninguna acción sobre ellas.
c. Las copias realizadas deberán realizarse en medios volátiles, es decir, en medios que no hayan contenido ningún dato anteriormente.289
d. En la medida de lo posible debe realizarse una copia exacta de la evidencia original para realizar los trabajos de investigación sobre la misma y no dañar los datos originales.

25. Indique cual de las siguientes herramientas no se suele usar en el análisis forense

a. Encase
b. Autopsy
c. FTK Imager
d. True Key

PRUEBA OBJETIVA TEÓRICA FINAL MF0488_3 : Gestión de Incidentes de Seguridad Informática			Fecha	07 / 08 / 2019
			Página 8 de 21	
Curso	SEGURIDAD INFORMATICA	**Código del curso**	18-38/000057	

BLOQUE DE ITEMS DE VERDADERO / FALSO

Para contestar a los ítems de Verdadero o Falso, en el recuadro de cada pregunta pon:

- "**V**" si consideras que es verdadera.
- "**F**" si consideras que es falsa.

Si te equivocas, táchala pon la respuesta que consideres correcta.

Cada ITEM tiene un valor de 1 punto

Fórmula de corrección: **Puntuación = Aciertos – Errores**

Calificación

26	27	28	29	30	31	32	33	34	35

26. Indique si la siguiente frase es verdadera o es falsa.

Los DoS son ataques de denegación del servicio. Estos ataques se realizan a equipos o a redes e impiden al usuario el acceso a un servicio o recurso determinado para el que está legitimado.

V	Verdadero32
	Falso

27. Indique si la siguiente frase es verdadera o es falsa.

Aunque la zona azul se considere zona de confianza y el tráfico analizado sea muy limitado, los IDS/IPS ubicados en esta zona no forman parte de la red interna del sistema, por lo que no se analizará el tráfico interno de la red.

	Verdadero40
	Falso

28. Indique si la siguiente frase es verdadera o es falsa.

Hay que diferenciar los sucesos de inicio de sesión de cuenta con los sucesos de inicio de sesión.

- [ ] Verdadero85
- [ ] Falso

29. Indique si la siguiente frase es verdadera o es falsa.

Los sucesos de inicio de sesión de cuenta hacen referencia a los intentos de acceso al equipo local a través de la red. Sin embargo, los sucesos de inicio de sesión son aquellos registrados cuando un usuario intenta iniciar la sesión desde el mismo equipo local.

- [ ] Verdadero85
- [ ] Falso

30. Indique si la siguiente frase es verdadera o es falsa.

Malware es el acrónimo en inglés de malicious y software, software malicioso. Forman parte de este grupo desde los clásicos virus hasta amenazas informáticas de lo más sofisticadas.

- [ ] Verdadero100
- [ ] Falso

31. Indique si la siguiente frase es verdadera o es falsa.

Los sistemas de detección de intrusiones (IDS) son un modo de protección reactiva ante intrusiones (medidas correctivas o reactivas), mientras que los sistemas de prevención de intrusiones (IPS) ejercen protección proactiva (medidas preventivas).

- [ ] Verdadero108
- [ ] Falso

32. Indique si la siguiente frase es verdadera o es falsa.

Los cortafuegos no protegen de los ataques originados desde dentro la red interna, por lo que es necesario implantar medidas de seguridad adicionales que impidan la expansión de intrusiones internas.

- [ ] Verdadero
- [ ] Falso

33.Indique si la siguiente frase es verdadera o es falsa.

En el momento de elaborar el Plan de Gestión de incidentes deberán proponerse medidas adicionales que se adapten a las características peculiares de cada sistema de información y organización.

- [ ] Verdadero156
- [ ] Falso

34.Indique si la siguiente frase es verdadera o es falsa.

La cadena de custodia de una evidencia es un procedimiento controlado de recolección y análisis de evidencias que tiene como finalidad la preservación de su integridad, evitando que su manejo no provoque vicios o alteraciones.

- [ ] Verdadero
- [ ] Falso

35. Indique si la siguiente frase es verdadera o es falsa.

A pesar de tener un impacto inferior que los intentos de entrada, los ataques enmascarados no deben subestimarse: su daño potencial puede ser igual o mayor que las otras intrusiones.

- [ ] Verdadero224
- [ ] Falso

BLOQUE DE ITEMS DE TEXTO INCOMPLETO

Para contestar a los ítems de completar, puedes poner en los espacios en blanco de la frase _____ el número que identifica a cada palabra.

(Fórmula de corrección : **Puntuación = Aciertos**

Calificación

36	37	38	39	40	41

36. Completa en los espacios las palabras que faltan :

La gestión de incidentes tiene como objetivo calcular y utilizar adecuadamente los _____2_____ necesarios para aplicar correctamente estas medidas de prevención, _____1_____ y corrección de incidentes de _____3_____.

1.	**DETECCIÓN**
2.	**RECURSOS**
3.	**SEGURIDAD**

37. Completa en los espacios las palabras que faltan :

Los registros de _____1_____ son aquellos en los que se registran las acciones realizadas por los _____3_____en un sistema. Estos registros son vitales para las organizaciones ya que cuando se produce un incidente de _____2_____ facilitan información sobre el usuario que haya podido cometer la infracción.

1.	**AUDITORIA**
2.	**SEGURIDAD**
3.	**USUARIOS**

38. Completa en los espacios las palabras que faltan :

Los gusanos o worms son programas _____2_____ diseñados con el fin de propagarse de un sistema a otro para degradar el _____1_____ de sus recursos.

1.	RENDIMIENTO
2.	AUTOCONTENIDOS

39. Completa la frase con las siguientes palabras :

Con la evaluación y análisis de todos los aspectos reflejados en el informe de verificación del _____2_____ ya se puede obtener una imagen global de por qué sucedió la _____1_____,qué es lo que ha quedado afectado, cómo se ha actuado al respecto y qué hay que _____3_____ para que no vuelva a ocurrir.

1.	INTRUSIÓN
2.	INCIDENTE
3.	MODIFICAR

40. Completa la frase con las siguientes palabras :

La ____2_____ de un incidente tiene como misión la __3_____de toda la información que pueda utilizarse para su resolución y para la _____1_____ del sistema.202

1.	RESTAURACIÓN
2.	CLASIFICACIÓN
3.	RECOPILACIÓN

41. Completa la frase con las siguientes palabras:

1.	TRATAMIENTO
2.	DIGITAL
3.	INFORMÁTICO

Una evidencia _____2_____, a diferencia de las evidencias físicas, es cualquier documento, fichero, registro, etc. que está contenido en un soporte _____3_____ o digital y que es susceptible de ____1_____.

BLOQUE DE ITEMS DE CORRESPONDENCIA

Para contestar a los ítems de correspondencia, puedes poner en LA COLUMNA EN BLANCO la letra que creas que corresponda.

(Fórmula de corrección : **Puntuación = Aciertos**

Calificación

42	43	44	45	46	47

42. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha: pag 13

A.	**MEDIDAS PREVENTIVAS**	**3**
B.	**MEDIDAS DE DETECCION**	**1**
C.	**MEDIDAS CORRECTIVAS**	**2**

1.	Medidas que sirven para detectar y controlar los incidentes de seguridad.
2.	Medidas implementadas una vez sucedido el incidente de seguridad que se utilizan para evitar que no vuelva a ocurrir y para restaurar el sistema la situación anterior a la incidencia.
3.	Medidas que se aplican para evitar la ocurrencia de incidentes de seguridad.

43. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha:

A.	**ERROR**	**1**
B.	**ADVERTENCIA**	**2**
C.	**INFORMACIÓN**	**3**
D.	**AUDITORIA CORRECTA**	**4**
E.	**AUDITORIA INCORRECTA**	**5**

1.	Para eventos de seguridad importantes.
2.	Para eventos que no son importantes pero que pueden causar algún problema en un futuro.
3.	Para operaciones realizadas con éxito.
4.	En eventos ocurridos cuando la auditoría se ha realizado correctamente.
5.	En eventos ocurridos cuando ha habido algún fallo de auditoría.

44. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha:

A.	**VIRUS**	**1**
B.	**TROYANOS**	**2**
C.	**COOKIES**	**3**

1.	Programas informáticos diseñados con la finalidad de producir algún tipo de daño en el equipo sin que el usuario se dé cuenta.
2.	Programas con funcionalidades ocultas diseñadas para fines maliciosos contra el usuario que los tiene instalados.
3.	Herramientas que no se consideran directamente una amenaza a los equipos pero que sí pueden vulnerar la confidencialidad y privacidad de los usuarios, ya que permiten a las webs el almacenamiento de los registros de cada visita de los usuarios.

45. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha: 173

A.	**CONTENCIÓN**	**1**
B.	**RECUPERACIÓN**	**2**
C.	**ERRADICACIÓN**	**3**

1.	Desconectar el equipo afectado de la red para impedir que se propague a los demás equipos.
2.	Restaurar el sistema dañado con la última copia de respaldo realizada con los datos del equipo.
3.	Localizar el virus y eliminarlo del equipo con la utilización de un antivirus.

46. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha: 199

A.	**ADMINISTRADOR DEL SISTEMA**	**1**
B.	**DESARROLLADORES Y ANALISTAS**	**2**
C.	**CENTRO DE SERVICIOS**	**3**

1.	Tienen un conocimiento más profundo del funcionamiento de las intrusiones y ataques y son los que realmente son capaces de desarrollar respuestas rápidas ante ataques más complejos.
2.	Tienen conocimientos avanzados sobre las posibles intrusiones que pueden acceder al sistema, su comportamiento y su funcionamiento interno. Pueden desarrollar herramientas de contraataque y protección avanzadas ante intrusiones desconocidas.
3.	Es el primer nivel de gestión de intrusiones, el punto de contacto entre los usuarios y la gestión de estas. Se encargan de dar soporte en la gestión realizando funciones como el registro y monitorización de incidentes y la aplicación de soluciones temporales y provisionales ante ataques e intrusiones, entre otras.

47. Relaciona las frases de la columna de la izquierda con las que creas que corresponda de la columna de la derecha: 270

A.	**PERSECUCION CRIMINAL**	**1**
B.	**MANTENIMIENTO DE LA LEY**	**2**
C.	**INVESTIGACION DE SEGUROS**	**3**

1.	La informática forense permite obtener evidencias que incriminen a los culpables de muchos tipos de delitos como, por ejemplo, fraudes financieros, tráfico de drogas, etc.
2.	La informática forense puede utilizarse también para llevar a cabo búsquedas iniciales en investigaciones con órdenes judiciales.
3.	La informática forense permite la recolección de evidencias que ayuden a las compañías de seguros a detectar estos casos de fraude y disminuir así sus costes.

BLOQUE DE ITEMS DE ENSAYO BREVE

Para contestar a los ítems de ensayo breve, hay que sintetizar la respuesta en a lo sumo tres frases.

(Fórmula de corrección : **Puntuación = Aciertos**

Calificación

48	49	50

48. En Usted, como responsable de seguridad de su organización, se encuentra en pleno proceso de definición de su política de seguridad. Ha estado evaluando las necesidades de la empresa y los requerimientos establecidos por la dirección y, finalmente, se ha decidido por un sistema que sea capaz de monitorizar el tráfico de red a tiempo real y que aplique medidas preventivas de modo automático. No le sirve la simple detección de las incidencias de seguridad.
pag 39

¿Qué tipo de sistema utilizaría: sistema de prevención de intrusiones o sistema de detección de intrusiones? ¿Por qué?

La herramienta que es capaz de monitorizar el tráfico de la red a tiempo real es el sistema de prevención de intrusos. Mientras que los IDS o sistemas de detección de intrusos se limitan a la simple detección de ataques (exitosos y no exitosos, según el tipo de IDS implantado), los IPS o sistemas de prevención de intrusos pueden aplicar medidas preventivas que eviten la entrada de ataques a tiempo real gracias a la monitorización de la red.

49. Usted, como administrador de la infraestructura de red de su empresa, está definiendo las políticas de corte de ataques ante detecciones de intrusiones del sistema IDS/IPS que pretende implantar. Quiere que el sistema, en cuanto detecte alguna intrusión, le envíe un SMS a su móvil indicando con detalle las características de la intrusión pero que no realice ninguna acción adicional automáticamente porque prefiere ser usted el que decida qué medida tomar en cada intrusión.

Pag 68

A) ¿De qué tipo de política de respuesta se está hablando en este caso?

Las políticas de respuesta ante detecciones de ataques que se limitan a notificar y a facilitar información detallada del ataque son las llamadas políticas de respuesta pasiva.

B) ¿Qué otras opciones de notificación de intrusión podría establecerse?

Otras opciones de notificación que se podrían establecer pueden ser el envío de correo electrónico, la apertura de una aplicación que genere una alerta o la notificación visual de una alerta, entre otras.

50. Usted, como responsable de seguridad, ha detectado que se ha producido una intrusión en uno de los equipos de la organización. La intrusión ha provocado el borrado de varios archivos importantes y, por ello, tiene previsto realizar un análisis forense para localizar al atacante y tomar medidas judiciales contra él.

A) ¿Qué tipo de ataque se ha producido y qué información deberá recopilar para reconstruir su secuencia temporal?

Pag 296

Al haberse producido borrado de información debido al ataque se deduce que se trata de un ataque activo (los ataques pasivos no modifican la información del equipo afectado, simplemente la "espían"). Para reconstruir su secuencia temporal y conocer el origen del ataque debería recopilarse la información siguiente de los ficheros eliminados y de los sospechosos:

\ Tamaño y tipo de los ficheros.
\ Usuarios y grupos a los que pertenecen los ficheros.
\ Permisos de acceso.
\ Detección de los ficheros eliminados.
\ Trazado de ruta completo.
\ Marcas de tiempo.