Grupo 10	Ejemplo Tercer Control de Seguretat Informàtica	Q1: 16-12-2019
Nombre:	Apellidos:	

Test. 4 puntos.
Tiempo de resolución estimado: **20 minutos**
Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.4 puntos.
- Multirespuesta (MR). Una respuesta MR correcta cuenta 0.4 puntos, la mitad si hay un solo error, 0 en los otros casos. En las MR puede haber desde una hasta todas respuestas correctas.

1. **RU**. Un fragmento de código que es capaz de ir reproduciéndose en programas hosts, modificando estos programas y dependiendo de sus ejecuciones

- ☐ Es un gusano
- ☐ Es un troyano
- ☐ Es un spyware
- ☐ Es un virus
- ☐ Es un botnet

2. **MR**. Identificar el/los ataque/s de tipo buffer overflow

- ☐ Agotar el espacio de memoria disponible atacando y matando los demás procesos
- ☐ Modificar el espacio de direccionamiento usado por el SO para acceder a los datos y procesos en ejecución en la memoria
- ☐ Ejecutar infinitos push para llenar el stack de datos inútiles
- ☐ Colar código extra en memoria durante una operación de lectura de datos del socket de red
- ☐ Ejecutar una función pasándole como argumento unos datos más grandes de lo esperado para sobrescribir parte de la memoria

3. **MR**. Marca la o las afirmaciones correctas acerca de la estructura de un SO

- ☐ Un dominio puede ser un usuario, un proceso o un procedimiento
- ☐ Si un proceso en el dominio D_i quiere hacer una operación *op* en el objeto O_j, entonces *op* debe estar en (i,j) de la matriz de acceso
- ☐ En una matriz de acceso se pueden añadir los objetos como dominios
- ☐ Una matriz de acceso suele ser pequeña y tener muchas casillas llenas

4. **RU**. La librería *crypt* se usa en Unix/Linux modernos para

- ☐ Cifrar una contraseña para su envío remoto
- ☐ Computar el hash de la contraseña de usuario junto al salt y guardarlo en el fichero shadow
- ☐ Cifrar las listas de acceso ACL donde se guardan los derechos de acceso de cada usuario
- ☐ Computar el hash de la contraseña de usuario y guardarlo en el fichero passwd

5. **MR**. Marca la o las afirmaciones correctas

- ☐ En España, no existen leyes especificas sobre Seguridad Informática
- ☐ Un incidente de seguridad solo puede ser investigado por vía civil
- ☐ Un CERT es un organismo público dedicado a buscar criminales cibernéticos
- ☐ El primer CERT se creó a partir del incidente del gusano Morris

6. **MR**. La cadena de custodia garantiza que

- ☐ Los resultados forenses de un análisis son fiables
- ☐ Una evidencia se pueda usar en procesos judiciales
- ☐ Las evidencias no han sido modificadas u alteradas
- ☐ Las evidencias han sido adquiridas de forma segura
- ☐ Todas las anteriores

7. **MR**. Un fichero LNK

- ☐ Proporciona información sobre varios usuarios
- ☐ Proporciona información sobre el volumen donde se almacena el fichero vinculado
- ☐ Se crea automáticamente al abrir un archivo
- ☐ Se encuentran tanto en sistemas de fichero Windows como en Linux

8. **MR**. Cuales de las siguientes afirmaciones sobre las evidencias son ciertas

- ☐ Éstas deben ser buscadas siempre y únicamente en los ordenadores y dispositivos de la víctima
- ☐ Cualquier dato puede ser una evidencia
- ☐ Hay que revisar el orden de registro u autorización legal para saber el alcance de la búsqueda de evidencias
- ☐ Cada evidencia precisa de un documento de cadena de custodia

9. **MR**. Forensic readiness consiste en

- ☐ Tener la capacidad de preservar, recopilar, proteger y analizar evidencias digitales de un posible incidente de seguridad
- ☐ Leer/analizar datos constantemente para determinar si hay un ataque, se está cometiendo un crimen, se está haciendo un mal uso de los recursos, etc.
- ☐ Saber preservar las evidencias digitales antes, durante y después de la ocurrencia del incidente
- ☐ Monitorizar los sistemas y usuarios: archivos de registro, correo electrónico, tráfico de red, llamadas telefónicas, etc.
- ☐ Aplicar los 5 puntos de una investigación forense: identificación, preservación, examinación, análisis y presentación

10. **MR.** Que sitios se suelen mirar a la hora de analizar un sistema Windows

- ☐ Papelera
- ☐ Ficheros prefetch
- ☐ Cola de impresión
- ☐ Registros de eventos
- ☐ Los metadatos ADS en el formato NTFS
- ☐ Archivos en el directorio /dev

Preguntas. 6 puntos, cada pregunta vale 1 punto.
Tiempo de resolución estimado: **35 minutos**.

1) Explicar **brevemente** que métodos se han implementado para protegerse de los ataques de tipo buffer overflow

2) Explicar **brevemente** el método de escaneo heurístico de los antivirus

3) Explicar **brevemente** que es una matriz de acceso en Unix/Linux y como funciona

4) Que circunstancias pueden motivar el inicio de un análisis forense

5) Explicar **brevemente** en que consiste la etapa de preservación en un análisis forense

6) Explicar **brevemente** en que consiste una imagen forense de un disco