Grupo 10	Tercer Control de Seguretat Informàtica	Q1: 20-12-2019
Nombre:	Apellidos:	

Test. 3 puntos.
Tiempo de resolución estimado: **20 minutos**
Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.3 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**. Se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante algún tipo de acceso remoto al equipo infectado

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

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

- ☐ Address Space Layour Randomization (ASLR) es una técnica usada en los antivirus modernos para detectar comportamientos anómalos
- ☐ Data Execution Prevention (DEP) dispone de forma aleatoria los datos de un proceso para prevenir posible ataque de tipo buffer overflow
- ☐ Least privilage es el principio que consiste en que los programas, usuarios y sistemas tengan los privilegios estrictamente suficientes para realizar sus tareas
- ☐ Weight-based system es un método de escaneo heurístico usado en los antivirus

3. **RU**. Que característica tienen los polymorphic virus

- ☐ Son virus capaces de propagarse por Internet
- ☐ Son virus capaces de auto-encriptarse
- ☐ Son virus capaces de recopilar información de un dispositivo y después transmite esta información a una entidad externa
- ☐ Son virus capaces de mutar cuando se reproducen de un host a otro
- ☐ Son virus que permiten un acceso de privilegio continuo a un ordenador pero que mantiene su presencia activamente oculta

4. **MR**. En un SO basado en matriz de acceso

- ☐ Cada objeto tiene una ACL adjunta que determina el dominio y los derechos de acceso
- ☐ Cada proceso tiene una lista de capacidades que le otorgan acceso a determinados objetos
- ☐ Si un objeto no tiene en su lista de capacidades una entrada para un determinado dominio, eso implica que no tiene ningún derecho para aquel dominio
- ☐ El SO usa la lista de capacidades para determinar si se puede abrir un objeto

5. **MR**. En una investigación forense, para la adquisición de una evidencia en un ordenador siempre hay que …

- ☐ Documentar el software/hardware que se van a utilizar
- ☐ Abrirlo delante de testigos
- ☐ Documentar los dispositivos de almacenamiento internos
- ☐ Revisar el orden de registro
- ☐ Desconectarlo de la red
- ☐ Realizar un clon de los dispositivos de almacenamiento

6. **MR**. Marca la o las afirmaciones correctas en relación con los ficheros prefetch

- ☐ Se pueden analizar para saber si se ha ejecutado un programa que ya no está instalado o ha sido borrado
- ☐ Windows escribe en estos ficheros ciertas características de las aplicaciones ejecutadas
- ☐ Sirven para acelerar la ejecución de las aplicaciones
- ☐ Son archivos de metadatos que contienen los detalles del archivo original

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

- ☐ En una adquisición Offline de un disco hay que bloquear la escritura antes de crear una copia
- ☐ La adquisición Live evita cambios debido al uso del equipo
- ☐ Se utiliza la adquisición Offline de un disco cuando este está encriptado
- ☐ La adquisición Live permite no perder datos volátiles

8. **MR.** Que sitios se suelen mirar a la hora de analizar un sistema Linux

- ☐ La información del sistema como /etc/host y /etc/shadow
- ☐ El histórico de comandos
- ☐ El fichero SAM
- ☐ Los datos y la información de configuración del usuario
- ☐ El registro de eventos /var/log

Grupo 10	Tercer Control de Seguretat Informàtica	Q1: 20-12-2019
Nombre:	Apellidos:	

Preguntas. 7 puntos.
Tiempo de resolución estimado: **35 minutos**.

1) (**1 punto**) Explicar **brevemente** los dos componentes de un gusano

2) (**1 punto**) Explicar **brevemente** en que consiste un ataque de tipo buffer overflow

3) (**1 punto**) Explicar **brevemente** en que consiste el orden de volatilidad en una investigación forense

4) (**1 punto**) Explicar **brevemente** en que consiste el forensic readiness

5) (**1.5 punto**) Enumerar las 6 etapas de una investigación forense y explicar con **una simple frase** en que consiste cada etapa

6) (**1.5 puntos**) Explicar **brevemente** que métodos/técnicas usan los antivirus modernos