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

- Replication: es la parte dedicada a la reproducción y distribución del gusano. Un gusano debe ser capaz de infectar equipos usando la red por lo tanto necesita acceder de forma remota a otro dispositivo, comprometiendo la cuenta de un usuario de alguna forma
- Payload: parte del código no dedicado a la reproducción y que se puede ejecutar en cualquier momento. Puede hacer cualquier tipo de daño según el tipo de acceso que tenga el usuario: cifrado de información, modificación/alteración de datos, buscar información, instalar un bot, etc.

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

La idea es aprovechar el mal uso del stack para pasar código malicioso a la memoria y posiblemente ejecutarlo. El ataque se verifica cuando se hace una operación se escritura en un buffer y no se controla el tamaño de lo que se escribe. Este buffer puede ser el stack que se usa al llamar una función que trate unos datos: si no se controla el tamaño de estos datos, se puede desbordar el stack y escribir datos adicionales como otras direcciones de vuelta o directamente código adicional. Este buffer también puede ser el buffer de recepción usado en un socket de red: al recibir unos datos remotos, se pueden pasar más datos de los esperado y colar algún dato o código adicional.

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

Durante la fase de adquisición, hay que preparar el orden de volatilidad (de mayor a menor), ordenando la información que se quiere adquirir según su disponibilidad en el tiempo: cuanto más volátil es una determinada posible evidencia (por ejemplo, memoria caché, tablas ARP, etc.), más urgente es adquirirla en el menor tiempo posible antes que desaparezcan.

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

Es la capacidad de una entidad de saber y poder preservar, recopilar, proteger y analizar evidencias digitales para que estas evidencias puedan ser utilizadas efectivamente: en cualquier asunto legal; en investigaciones de seguridad; en procedimientos disciplinarios; en un tribunal laboral; o en un tribunal de justicia

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

- Identificación del escenario: evaluar, acotar y asegurar el entorno en el que se ha producido el crimen
- Preservación: documentar exhaustivamente la metodología que se empleará para la búsqueda de las evidencias
- Adquisición: recuperar las evidencias según el orden de volatilidad
- Examinación: agregar, filtrar y sacar la información relevante de todo lo que ha adquirido
- Análisis: analizar las evidencias en un entorno de laboratorio para sacar conclusiones demostrables y reproducibles
- Presentación: elaboración de un informe y presentación del mismo

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

Los antivirus modernos usan varios métodos/técnicas para detectar códigos maliciosos:

- Método basado en firmas: se escanean los ficheros en busca de determinadas firmas, es decir trozos de códigos determinados que se sabe pertenecen a virus conocidos (virus definition tables)
- Escaneo heurístico basados en pesos: se califica cada funcionalidad con un cierto peso de acuerdo al daño que puede causar; se considera que un código es malicioso si la suma de sus pesos pasa de un determinado umbral
- Escaneo heurístico basados en reglas: se compara el comportamiento de un código con determinadas reglas que se sabe usan los códigos maliciosos
- Escaneo heurístico en maquinas virtuales: al ejecutar un programa, este se lanza primero en una maquina virtual aislada para analizar su comportamiento; si no se detecta nada anómalo, se procede a su ejecución en la maquina real

  Este último incluye la búsqueda de patrones típicos de códigos maliciosos encriptados