1. Dibuja un diagrama que muestre el proceso de traducción de dirección lógica a dirección física para una arquitectura Intel x86 (PAE incluido, mostrando el nombre de las diferentes direcciones que toman parte en dicho proceso). (1.45 p.)
2. Qué diferencia hay entre dirección virtual y dirección física? (0.25 p.)
3. Qué diferencia hay entre un binario y un proceso? (0.25 p.)
4. Cómo es posible que cada proceso tenga el mismo espacio de direcciones? (0.25 p.)
5. En qué dos “conceptos” está dividido un PE y qué representan? (0.25 p.)
6. Qué significa que un binario esté dinámicamente o estáticamente enlazado? Qué inconvenientes tiene que un binario esté estáticamente enlazado a la hora de hacer un análisis estático? (0.25 p.)
7. Explica lo que es un “import”? (0.25 p.)
8. Explica lo más detallado posible qué significa “resolver un import”? (0.5 p.)
9. Por defecto, en un PE, cuando se resuelven los imports? (0.225 p.)
10. Por defecto, en un ELF, cuando se resuelven los imports? (0.225 p.)
11. De toda la estructura de datos de un PE, enumera y explica dos campos. (0.35 p.)
12. Enumera y explica dos secciones ya sea de un PE, un ELF o de ambos. (0.35 p.)
13. Explica qué son las secciones y segmentos de un ELF y en qué se diferencian? (0.25 p.)
14. Como utilizan los creadores de malware las siguientes features de los PE:
    a. Resources (0.125 p.)
    b. TLS Callbacks (0.125 p.)
15. Qué harías para identificar qué tipo de fichero es un fichero que te han proporcionado sin extensión? (0.25)
16. Enumera cuatro herramientas que conozcas para hacer análisis estático de binarios y defínelas usando tus propias palabras. (0.25)
17. Qué ventaja tiene usar la instrucción “lea” en vez de “mov”? (0.2p)
18. Para qué se utiliza la instrucción “xor eax, eax”? [nota: La respuesta “hacer una xor entre eax y eax” no es válida”] (0.2p)
19. Qué es el stack de un proceso? Para qué se utiliza? (0.4p)
20. Qué es un stack frame? (0.2p)
21. Dibuja un stack frame una vez se acaba de llamar a una función X. (1p)
22. Qué es un calling convention? (0.4p)
23. Enumera tres calling conventions y para uno de ellos explica: (0.4p)
    a. Cómo se gestionan los parámetros (en el prólogo y epílogo de una función).
    b. Cómo se gestiona el valor de retorno.
24. Enumera 3 herramientas que usarías (y para qué) para analizar dinámicamente el comportamiento de un binario. [nota: nombra como máximo un debugger] (0.4p)
25. Enumera todas las etapas a nivel de post-explotación tal y como se detallan en MITRE ATT&CK. (0.4p)
26. Qué método de persistencia se utilizaba en el sample de wannacry que analizamos en clase? (0.4p)
27. Qué técnica usaba el sample de wannacry para droppear un binario? (0.4p)