1. Qué ventaja tiene usar la instrucción “lea” en vez de “mov”? (0.2p)
2. Para qué se utiliza la instrucción “xor eax, eax”? [nota: La respuesta “hacer una xor entre eax y eax” no es válida”] (0.2p)
3. Qué es el stack de un proceso? Para qué se utiliza? (0.2p)
4. Qué es un stack frame? (0.2p)
5. Dibuja un stack frame una vez se acaba de llamar a una función X. (0.5p)
6. Qué es un calling convention? (0.2p)
7. Enumera tres calling conventions y para uno de ellos explica: (0.2p)
    a. Cómo se gestionan los parámetros (en el prólogo y epílogo de una función).
    b. Cómo se gestiona el valor de retorno.
8. Enumera 3 herramientas que usarías (y para qué) para analizar dinámicamente el comportamiento de un binario. [nota: nombra como máximo un debugger] (0.2p)
9. Enumera todas las etapas a nivel de post-explotación tal y como se detallan en MITRE ATT&CK. (0.2p)
10. Qué método de persistencia se utilizaba en el sample de wannacry que analizamos en clase? (0.2p)
11. Qué técnica usaba el sample de wannacry para droppear un binario? (0.2p)