1. **Qué ventaja tiene usar la instrucción “lea” en vez de “mov”? (0.2p)**

Con “lea” a parte de asignar un valor de un registro a otro registro, usando la misma instrucción se pueden realizar operaciones aritméticas sobre el valor del registro origen. Por ejemplo:

- lea eax, [edx+0x10]

Con una instrucción “mov” se debería utilizar más de una instrucción para conseguir lo mismo.

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)**

Para almacenar un 0 en el registro eax.

3. **Qué es el stack de un proceso? Para qué se utiliza? (0.2p)**

El stack es una región de memoria dentro de un proceso. Se utiliza para gestionar las llamadas a funciones.

4. **Qué es un stack frame y para qué sirve? (0.2p)**

Un stack frame es una estructura de datos que sirve para almacenar los datos necesarios para la ejecución de una función.

5. **Dibuja un stack frame una vez se acaba de llamar a una función X. [nota: no importa el calling convention] (0.5p)**

High memory address

Param 1
Param 2
Param N
Saved EIP address
Saved EBP address
Local var 1
Local var 2
Local var N

Low memory addresses

6. **Qué es un calling convention? (0.2p)**

Un calling convention es el proceso que se sigue cuando se llama y cuando se sale de una función. El calling convention define cómo se almacenan los parámetros en la pila, cómo se almacena el valor de retorno de la función, como se limpian los parámetros de la pila, etc.

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.**

cdecl, stdcall, fastcall.

	cdecl
Prologue	**Caller** pushes params to stack right to left.
Return Value	Stored in eax.
Epilogue	**Caller** cleans up parameters.

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)**

- Process Explorer: Identificar qué procesos se están ejecutando en el sistema en un momento dado. Ver también qué librerías ha cargado y qué handles se han abierto.
- RegShot: Hacer diffs del registro/archivos antes y después de ejecutar un binario.
- Process Monitor: Registrar multiples eventos que ocurren en el sistema operativo y filtrarlos, de modo que pueda identificar, por ejemplo, qué archivos ha creado un binario, qué conexiones se han iniciado, qué claves de registro se han leído, etc.

9. **Enumera todas las etapas a nivel de post-explotación tal y como se detallan en MITRE ATT&CK. (0.2p)**

Persistence, privilege escalation, credential access, defense evasion, execution, discovery, lateral movement, collection, exfiltration, command and control.

La semana pasada se añadió “initial access”.

10. **Qué método de persistencia se utilizaba en el sample de wannacry que analizamos en clase? (0.2p)**

Creaba un servicio de windows que iba a ejecutarse a si mismo (con varios parámetros) cada vez que se reiniciaba el sistema. Además, el servicio se ejecutaba una vez se había creado.

11. **Qué técnica usaba el sample de wannacry para droppear un binario? (0.2p)**

Wannacry tenía un binario PE embebido como un “resource”. El propio sample de wannacry que analizamos leía ese “resource” y lo escribía en el disco.