Name: ID:

Malware – Master on Cybersecurity

Final Exam, January 12th 2023

- This exam is individual, you cannot receive any external help to perform it. Use of any external source will be punished.
- Don't forget to specify your full name and Identity Card number on top of this page. You **don't** need to do that for all the pages of the exam.
- The exam is marked from 0 to 10, where 0 is no correct answer and 10 is the perfect exam.
- Each question has its value indicated with all the subsections' values as well.
- The exam may be resolved using one of the following languages:
  - Catalan
  - Spanish
  - English

It is mandatory to explain and develop all your answers to get the full punctuation, just answering yes or no will obtain 0 points. An exception to this is the test, where marking the correct answer is enough.

Duration: 1 hour and 55 minutes (No extension will be granted)

Question 1 (4 points)

Answer the following questions regarding infection propagation lesson.

1. Given the following assembly code and its translation to binary format:

```
global _start
_start:
eb 27           jmp short ender
starter:
48 31 c0        xor rax, rax
48 31 db        xor rbx, rbx
48 31 d2        xor rdx, rdx
b9 00 00 00 00  mov ecx, 0
b8 01 00 00 00  mov eax, 1 ; write
bf 01 00 00 00  mov edi, 1
```

```
5e              pop rsi
ba 06 00 00 00  mov edx, 6
0f 05           syscall
48 31 c0        xor rax, rax
b0 3c           mov al, 60    ; exit
48 31 ff        xor rdi, rdi
0f 05           syscall
ender:
e8 d1 ff ff ff  call starter
48 65 6c 6c 6f  db 'Hello', 0x0a, 0x00
         0a 00
```

(0.75 Points)

Indicate if it could be used as shellcode. If not, indicate which changes should be done to make it so and why:

2. Describe how Stack overflows leverage the stack to perform an attack and which mitigation techniques are used by compilers and operating systems. **(0.75 Points)**

3. When creating shellcode for windows which is the main issue we find when we want to execute syscalls such as MessageBoxA? **(0.75 Points)**

4. Why ROP is able to bypass most of security measures set by compilers when overflowing buffers? **(0.75 Points)**

5. Describe the three different mechanisms we studied to infect binaries and their differences. **(1 Points)**

Question 2 (2 points)

1. Describe how would you fool a linear sweep disassembler: **(0,5 Points)**

2. Describe what is a metamorphic virus and its advantages in respect to other types **(0.5 Points)**

3. How can a virus know it is being run on a Virtual Machine? **(0.5 Points)**

4. To fool recursive traversal, we can use techniques such as placeholder building. Explain what it entitles, how it works and why is able to fool recursive traversal? **(0.5 Points)**

Question 3 (2 points)

Answer the following theoretical questions

1. Describe the OWASP Top 10 vulnerability: **A04:2021 – Insecure Design**. **(0.5 Points)**

2. Explain how a user-mode rootkit works and how it differentiates from a Trojan horse. **(0.5 Points)**

3. Discuss about worms, their life-cycle and how they propagate. **(0.5 Points)**

4. From OWASP Top 10 describe the vulnerability **A01:2021 – Broken Access Control** and why it is the number one currently. **(0.5 Points)**

Question 4 (2 points)

Answer the following question marking the appropriate cell. Each question has only one valid response.

Each correct answer gives 0.5 points. WRONG ANSWERS SUBTRACT 0.25 points, you can decide to leave blank answers. The minimum punctuation for the test is 0 (it doesn't affect the punctuation of other questions).

1. Regarding buffer overflows:
   - □ a) Through specific input to the application they abuse memory allocation bugs and optimizations to own buffers, leading to potential arbitrary code execution.
   - □ b) By particular input to the application they affect the stack, disrupting them and potentially leading to arbitrary code execution.
   - □ c) By overflowing the heap, using specific input to the application, they lead to application crashes and potential arbitrary code execution.

2. Which of the following is an anti-emulation technique?
   - □ a) Count the cycles necessary to execute simple instructions
   - □ b) Use placeholders
   - □ c) Use XOR obfuscation

3. From OWASP, the Injection vulnerability group:
   - □ a) Refers only to SQL injection, where we are able to attack wordpress
   - □ b) Refers to any kind of injection, where SQL is the most frequent nowadays
   - □ c) Is a technique by which we inject code into an application with the final goal of overflowing the buffers

4. Which is the most critical aspect of an antivirus regarding stability?:
   - □ a) The antivirus database, as it is the block in charge of threat detection.
   - □ b) The engine, since it is the brains of the operation.
   - □ c) The engine, which is the one in charge of parsing the files on disk.