Name: ID:

A

MALWARE

Lab Exam, December 21st 2022

This exam is individual, we will validate if there are copies, if found we will take the proper measures

You cannot use books or any other supporting material.

Don't forget to indicate your full name and passport or ID number in this page.

Duration: 30 minutes (There will not be any time extension)

Answer the following questions marking the correct answer. There is only one valid answer for each question.

Consider that each correct answer gives 0.5 points. WRONG ANSWERS DISCOUNT 0.25 points.

1. In Linux when we want to hide a process we can:
   - ☐ a) Preload a library which modifies relevant system calls, hence allowing to fully bypass libc.
   - ☐ **b) Preload a library which proxies the invocation to relevant functions bypassing the desired process to hide it.**
   - ☐ c) It is not possible to hide processes at userspace, since the kernel is the sole responsible to keep the processes double linked list.

2. When we want to hide a process in Windows
   - ☐ **a) One mechanism is to modify the kernel linked list bypassing the desired process, but this does not work very well because Windows is able to detect the change because it keeps two different lists**
   - ☐ b) One mechanism is to modify the kernel linked list bypassing the desired process, but this does not work very well because Windows controls the values of the internal structures and keeps them read-only
   - ☐ c) We just modify the Task Manager syscalls with fake ones that allow to bypass the entry

3. When we want to access a DLL in a windows binary using shellcode
   - ☐ a) It is not possible to do this in windows, since the PE file loader is protected by the kernel
   - ☐ b) We have to look for the position of the LoadLibrary call by using the FS segment and moving to the position of ntdll.dll and from there accessing the library
   - ☐ **c) We have to look for the position of the LoadLibrary call by using the FS segment and moving to the position of kernel32.dll and from there accessing the library**

4. When we invoke a syscall in Linux using 64bit which of the following is **FALSE**?
   - ☐ a) RAX contains the number of syscall we want to invoke, other registers are used as parameters and the return value is stored in RBX
   - ☐ **b) RAX contains the number of syscall we want to invoke, the first parameter is passed using the RDI register**
   - ☐ c) Each syscall has a number assigned to it, it can vary from architecture to architecture

5. Why when a stack Overflow occurs the application normally crashes?
   - ☐ a) Always when overflowing a buffer we write to incorrect memory positions, causing a page fault and the subsequent crash
   - ☐ b) Normally it does not crash, the reason being the compiler setting up guards to avoid it
   - ☐ **c) It crashes because both RBP and RIP are overwritten, hence accessing to probably incorrect memory locations on function return**

6. Why buffer (or stack) overflows happen?
   - ☐ **a) Because of bad development practices where no boundaries are checked**
   - ☐ b) Because of lazy developers
   - ☐ c) Misdesigned programming languages that allow them

7. Which are the implications of ASLR on the overflow
   - ☐ a) None, since it is disabled by default
   - ☐ **b) The memory randomization causes the overwriting of RIP to point to wrong memory positions**
   - ☐ c) ASLR stands for Address Space Layout Rendering, which permits to render invalid buffer overflows, consequenty making the system perfectly secure

8. What is a NOP sled?
   - ☐ a) Is a series of \x90 instructions which do exactly nothing, so it's pointless
   - ☐ b) It is a security technique by which we invalidate malware bytes using NOPs
   - ☐ **c) It is a series of NOP that give more margin to the memory position where to return within the stack when dealing with stack overflows**

9. When a Virus infects a binary file on Windows
   - ☐ a) It has to necessarily add a new section and modify the Entrypoint of the executable
   - ☐ b) When it adds a new section, it can use more bytes to contain the virus and hence pass unnoticed, as it acts as an obfuscation technique as well
   - ☐ **c) Adding a new section is the most flexible way of creating a virus, but sadly it is easier to detect because the filesize will always change**

10. Which of the following codes fools linear debuggers?

☐ a)
```
mov eax, [eax+0x00c]
mov esi, [eax+0x014]
lodsd
```

☐ **b)**
```
push rbx
jmp short 4
db 0x57,0x48, 0xe3
lodsd
```

☐ c)
```
xor rax, rax
mov al, 60
xor rdi, rdi
syscall
```

11. When obfuscating malware, if using instruction placeholders to embed code, which considerations do we need to take into account?
    - ☐ **a) We have to pad with NOPs the holes**
    - ☐ b) Performance
    - ☐ c) Anti-emulation techniques

12. Which of the following shellcodes guaranties running the exit (code 60) system call in Linux with a 0 exit code?

*** Assume that initially all registers are initialized to 0xFFFFFFFFFFFFFFFF**

☐ a)
```
mov al, 60
xor rdi, rdi
syscall
```

☐ b)
```
xor rax, rax
xor rbx, rbx
mov al, 60
syscall
```

☐ **c)**
```
xor rax, rax
mov al, 60
xor rdi, rdi
syscall
```

13. Which of the following is the most correct answer when considering an XOR encryptor?
    - ☐ **a) We first decide the encryptor key, we then add junk instructions, finally we encrypt**
    - ☐ b) We first decide the encryptor key, then we encrypt, finally we add junk instructions
    - ☐ c) It doesn't matter, both are correct

14. Indicate the most accurate consideration when inserting junk code to a virus
    - ☐ a) Junk code is useless, as a consequence it can be added anywhere in a virus payload as long as it uses unused registers
    - ☐ b) We can only use unused registers to avoid breaking the virus semantics
    - ☐ **c) We have to be careful about the flow control (jumps) as they may vary**

15. On a XOR encrypted virus, where the Antivirus centers its detection?
    - ☐ a) They are undetectable with signatures, we have to rely on behavioral analysis
    - ☐ **b) To be reliable it will center on the decoding loop**
    - ☐ c) It is centered on the payload, since XOR is easily breakable

16. Which of the following is a correct pattern matching for ClamAV?
    - ☐ **a) NewVirus;Target:6;(0&1&2);4d31c0;41b1;eb1a584831c948**
    - ☐ b) <virus name="NewVirus"><pattern mode="hex">eb1a584831c948</pattern></virus>
    - ☐ c) eb1a584831c948; 4d31c0;41b1;NewVirus;(0&1&2)

17. In the Ethical Hacking Lab, there was this Brute Force attack. To do it we could use different applications, which of the following may apply to the case of the lab?
    - ☐ a) John The Ripper
    - ☐ **b) Hydra**
    - ☐ c) nmap

18. In the DVWA, the challenge of the command injection required to add a command in a particular way, how did we scape in the beginner level the Ping to be able to execute arbitrary commands?
    - ☐ **a) We used ; followed by the command**
    - ☐ b) We had to use a null byte to be able to escape
    - ☐ c) As a regular SQL injection we had to play a little bit with ' and SELECT statements

19. In Ethical Hacking lab we had the challenge of the File Upload, where the goal of the beginner level was:
    - ☐ a) To execute arbitrary Bash commands
    - ☐ b) That challenge was not part of the lab
    - ☐ **c) To execute arbitrary PHP functions**

20. A Christmas present, which lab was more fun?
    - ☐ **a) Process Hiding**
    - ☐ **b) Stack Overflow + Virus creation**
    - ☐ **c) Code obfuscation**
    - ☐ **d) Ethical Hacking**
    - ☐ **e) Antivirus**