X

Week 1 : Assignment 1

The due date for submitting this assignment has passed.

Due on 2025-02-05, 23:59 IST.

Assignment submitted on 2025-02-04, 22:14 IST

1) Which of the following sections in an ELF file contains the executable machine code? ***1 point***

- `.text`
- `.data`
- `.bss`
- `.symtab`

Yes, the answer is correct.
Score: 1
Accepted Answers:
`.text`

2) Which of the following is a common cause of buffer overflow vulnerabilities in software? ***1 point***

- Using dynamically allocated memory.
- Writing more data to a buffer than it can hold.
- Declaring global variables in a program.
- Using high-level programming languages like Python or Java.

Yes, the answer is correct.

Score: 1
Accepted Answers:
Writing more data to a buffer than it can hold.

3) Consider the following C program:

```
#include <stdio.h>
#include <string.h>

int main() {
    char buffer[10];
    strcpy(buffer, "HelloWorldOverflow");
    printf("Buffer contains: %s\n", buffer);
    return 0;
}
```

If the **`buffer`** array can hold 10 characters, how many extra characters are written to memory due to the **`strcpy`** operation?

8

No, the answer is incorrect.
Score: 0
Accepted Answers:
(Type: Numeric) 9

1 point

4) Match the following ***1 point***

A) .data	1) Stores uninitialized global and static data
B) .bss	2) Stores initialized global and static variables
C) .symtab	3) Stores read-only data like string literals
D) .rodata	4) Stores the symbol table for debugging

- A-1 B-2 C-4 D-3
- A-1 B-3 C-2 D-4
- A-2 B-1 C-3 D-4
- A-2 B-1 C-4 D-3

No, the answer is incorrect.
Score: 0
Accepted Answers:
A-1 B-2 C-4 D-3

5) You are debugging a program in GDB and you have stopped at a breakpoint. The value of a variable **`x`** is **`0x1000`**, and the program counter (PC) is at address **`0x2000`**. If you use the GDB command **`x/4xw $pc`**, what will be the output? ***1 point***

- The contents of 4 words starting from address **`0x2000`**.
- The contents of 4 bytes starting from address **`0x2000`**.

(unit?unit=17&lesson=26)

Quiz: Week 1 : Assignment 1 (assessment?name=145)

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Download Videos ()

Text Transcripts ()

Books ()

Lecture Material ()

- The contents of 4 words starting from address `0x1000`.
- The contents of 4 bytes starting from address `0x1000`.

Yes, the answer is correct.
Score: 1
Accepted Answers:
The contents of 4 words starting from address `0x2000`.

6) In the context of exploiting a buffer overflow vulnerability, which of the following is a key characteristic of shellcode that makes it effective for executing arbitrary commands on a target system? ***1 point***

- Shellcode is typically written in a high-level language, making it portable across different architectures.
- Shellcode is designed to run correctly regardless of where it is placed in memory.
- Shellcode relies on external libraries to execute system calls, making it vulnerable to detection by security tools.
- Shellcode is executed by the operating system's kernel, bypassing user-space security mechanisms like stack canaries.

Yes, the answer is correct.
Score: 1
Accepted Answers:
Shellcode is designed to run correctly regardless of where it is placed in memory.

7) True or False: ***1 point***

The GCC flag `-fno-stack-protector` helps prevent buffer overflow vulnerabilities by disabling stack protection mechanisms.

- True
- False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

8) In a 32-bit system, we are debugging a program using gdb, and we run the following command ***1 point***

$ x/32x $esp,

what is the size of the memory displayed in bytes?

- 1 byte
- 1024 bytes
- 128 bytes
- 32 bytes

Yes, the answer is correct.
Score: 1

Accepted Answers:
128 bytes

9) Suppose the above program is compiled as follows: ***1 point***

$ gcc prog.c –o prog

Which of the following statements will display the contents of executable sections?

- objdump -d -Mintel prog
- objdump --disassemble-all prog
- objdump --disassemble prog.c
- objdump -D prog

No, the answer is incorrect.
Score: 0

Accepted Answers:
objdump -d -Mintel prog

10) Match the following ***1 point***

1. Instructions	a. Heap section
2. Global and Static Data	b. Stack section
3. Function call invocation	c. Data section
4. Dynamic allocation	d. Text section

- 1-d 2-c 3-b 4-a
- 1-a 2-b 3-c 4-d
- 1-d 2-d 3-c 4-a
- 1-a 2-b 3-d 4-c

Yes, the answer is correct.
Score: 1

Accepted Answers:
1-d 2-c 3-b 4-a