X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

harshith.savanur01@gmail.com

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Information Security - 5 - Secure Systems Engineering (course)

Click to register for Certification exam (https://examform.nptel.ac.in/2025_01/exam_form/dashboard)

**If already registered, click to check your payment status**

Course outline

**About NPTEL ()**

**How does an NPTEL online course work? ()**

**Week 1 ()**

**Week 2 ()**

- Preventing buffer overflows with canaries and W^X (unit?unit=27&lesson=28)

# Week 2 : Assignment 2

**The due date for submitting this assignment has passed.**

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

## Assignment submitted on 2025-01-31, 08:33 IST

For **Question 1 and 2** consider the following code

```
int main(int argc, char **argv)
{
    char Copy[128];
    char *pA = argv[2];
    char *pC = Copy;
    int i = atoi(argv[1]);
    int j = 0;

    while (i-- && j < 128)
    {
        *(pC + j++) = *(pA + i);
    }

    return 0;
}
```

The program is compiled using the below command

```
gcc -o main main.c
```

1) Which of the following executions of the program causes the program to crash? ***1 point***

○ ./main 50 ExampleString

- Return-to-libc attack (unit?unit=27&lesson=29)
- ROP Attacks (unit?unit=27&lesson=30)
- Demonstration of Canaries, W^X, and ASLR to prevent Buffer Overflow Attacks (unit?unit=27&lesson=31)
- Demonstration of a Return-to-Libc Attack (unit?unit=27&lesson=32)
- Demonstration of a Return Oriented Programming (ROP) Attack (unit?unit=27&lesson=33)
- Week 2 Feedback Form : Information Security - 5 - Secure Systems Engineering (unit?unit=27&lesson=34)
- **Quiz: Week 2 : Assignment 2 (assessment?name=146)**

**Week 3 ()**

**Week 4 ()**

**Week 5 ()**

○ ./main 12 SecureSystemsEngineering

○ ./main 128 HelloWorld

● ./main 50000 InformationSecurity

Yes, the answer is correct.
Score: 1

Accepted Answers:
*./main 50000 InformationSecurity*

2) What is the vulnerability present in the program? ***1 point***

○ Buffer overflow

● Out-of-bounds memory access

○ Vulnerability in linux kernel

○ There is no vulnerability

Yes, the answer is correct.
Score: 1

Accepted Answers:
*Out-of-bounds memory access*

3) In a Return-Oriented Programming (ROP) attack, which of the following statements is **true** about ROP gadgets? ***1 point***

● ROP gadgets are short sequences of machine instructions that end with a return instruction (`ret`) and can be chained together to perform arbitrary computations.

○ ROP gadgets are used to directly execute shellcode by jumping to a specific address in memory.

○ The main purpose of ROP gadgets is to overwrite the return address with a system call address to execute malicious code.

○ ROP gadgets are only effective when the program is compiled with no stack protection mechanisms such as Stack Canaries.

Yes, the answer is correct.
Score: 1

Accepted Answers:
*ROP gadgets are short sequences of machine instructions that end with a return instruction (`ret`) and can be chained together to perform arbitrary computations.*

4) Which of the following GCC options provides protection against buffer overflows by adding stack canaries to detect stack-based buffer overflow attacks? ***1 point***

○ -fno-stack-protector

● -fstack-protector-all

○ -D_FORTIFY_SOURCE=2

○ -fPIC

Yes, the answer is correct.
Score: 1

Accepted Answers:
*-fstack-protector-all*

**Week 6 ()**

**Week 7 ()**

**Week 8 ()**

**Download Videos ()**

**Text Transcripts ()**

**Books ()**

**Lecture Material ()**

5) Which of the following is **necessary** for a **Return-to-libc (ret2libc)** attack to successfully execute a system command such as `system("/bin/sh")`? ***1 point***

○ The attacker must overwrite the return address with the address of the `exit()` function in libc.

● The attacker needs to control the argument passed to a function like `system()` to execute arbitrary commands.

○ The attacker must inject their own shellcode into the program's memory to call `system("/bin/sh")`.

○ The attacker must disable Data Execution Prevention (DEP) to execute shellcode.

Yes, the answer is correct.
Score: 1

Accepted Answers:
*The attacker needs to control the argument passed to a function like `system()` to execute arbitrary commands.*

6) True or False: In a Return-Oriented Programming (ROP) attack, the attacker can exploit system architectures like RISC and CISC equally, since ROP relies on chaining existing instruction sequences (gadgets) that end with a ret instruction, which is supported in both architectures. ***1 point***

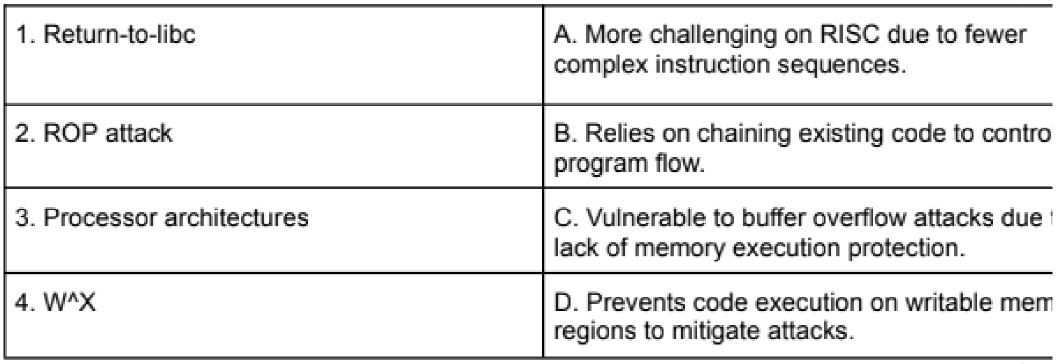
○ True

● False

Yes, the answer is correct.
Score: 1

Accepted Answers:
*False*

7) Match the following ***1 point***



| | |
|---|---|
| 1. Return-to-libc | A. More challenging on RISC due to fewer complex instruction sequences. |
| 2. ROP attack | B. Relies on chaining existing code to contro program flow. |
| 3. Processor architectures | C. Vulnerable to buffer overflow attacks due t lack of memory execution protection. |
| 4. W^X | D. Prevents code execution on writable mem regions to mitigate attacks. |

○ 1:A 2:B 3:C 4:D

○ 1:C 2:B 3:A 4:D

○ 1:B 2:C 3:D 4:A

● 1:D 2:A 3:B 4:C

No, the answer is incorrect.
Score: 0

Accepted Answers:
*1:C 2:B 3:A 4:D*

8) In a **ROP attack**, the attacker often targets the ________ to overwrite it with the address of a desired **gadget**, allowing them to control the program's execution flow and perform arbitrary operations. ***1 point***

○ Stack pointer

● Return address

○ Program counter

○ Instruction pointer

Yes, the answer is correct.
Score: 1

Accepted Answers:
*Return address*

9) In a **ROP attack**, if an attacker constructs a chain of 4 gadgets, and the first gadget is located at address 0x601000, with each gadget being 12 bytes in size, the address of the fourth gadget in the chain will be ———— (use hexadecimal notation in lowercase) ***1 point***

○ 0x621330

○ 0x601300

● 0x601030

○ 0x501130

Yes, the answer is correct.
Score: 1

Accepted Answers:
*0x601030*

10) Which of the following is **true** about exploiting a buffer overflow using **Return-Oriented Programming (ROP)?** ***1 point***

○ ROP attacks require the attacker to inject custom shellcode into the program's memory to execute arbitrary code.

● In a ROP attack, the attacker overwrites the return address with the address of existing functions or instruction sequences in the program’s memory, allowing the execution of arbitrary code.

○ ROP attacks only work on programs with non-executable stacks.

○ ROP attacks exploit buffer overflows by executing injected code directly from the stack.

Yes, the answer is correct.
Score: 1

Accepted Answers:
*In a ROP attack, the attacker overwrites the return address with the address of existing functions or instruction sequences in the program’s memory, allowing the execution of arbitrary code.*