Thomas Jun Wei Lim (username: tjwlim)

Attempt 7

Written: Feb 2, 2017 12:13 PM - Feb 2, 2017 12:14 PM

Submission View

Your quiz has been submitted successfully.

🛑 **Information**

Choose the best answer.

Questions

Question 1   1 / 1 point

Which of the following animals has no relation to computer security:

○ Worms

○ Rabbits

⦿ Llamas

○ Horses

○ Pigs

> View Feedback

Question 2   1 / 1 point

Which of the following is not a channel through which information can be sent covertly:

○ Storage

○ File Locks

⦿ /dev/null

○ Blocking

○ Graphics

> View Feedback

Question 3   1 / 1 point

Which of the following statements about incomplete mediation is true:

1. It is security hole for the server to rely on client data without checking for errors.
2. It is difficult to usefully exploit.
3. It is has only recently become important in security.
4. It is seldom an intentionally malicious program flaw.

○ 1

○ 1 and 2

○ 1, 2 and 3

○ 1, 3, and 4

◉ 1 and 4

> View Feedback

Question 4   1 / 1 point

Finding a security hole and patching the hole, known as penetrate and patch, fails for the following reasons:

1. Concern to resolve an outstanding bug results in an insular focus that ignores underlying causes of specific manifestations of penetrable software.
2. Security audits of software are expensive, time consuming, and not cost-effective.
3. Security holes often afflict poorly designed software that is hard to modify without causing more errors or impacting performance.
4. Regardless of the patched security holes, attackers will always find a way to penetrate the system.

○ 4

○ 1 and 2

◉ 1 and 3

○ 1, 2, and 3

○ 2, 3, and 4

> View Feedback

Question 5   1 / 1 point

What is the buffer-overflow related concern with regards to the following C library function: char* gets(char*);

○ The buffer size provided to the method may be incorrect.

◉ The function will not check against a buffer size.

○ When used inside a loop, a programmer may forget to consider the buffer size.

> View Feedback

Question 6   1 / 1 point

What is the buffer-overflow related concern with regards to the following C library function: char *fgets(char *, int, FILE*);

◉ The buffer size provided to the method may be incorrect.

○ The function will write past the buffer size provided.

○ When used inside a loop, a programmer may forget to consider the buffer size.

> View Feedback

Question 7   1 / 1 point

What is the buffer-overflow related concern with regards to the following C library function: int getc(FILE*);

○ The buffer size provided to the method may be incorrect.

○ The function will write past the buffer size provided.

◉ When used inside a loop, a programmer may forget to consider the buffer size.

> View Feedback

Question 8   1 / 1 point

What is the buffer-overflow related concern with regards to the following C library function: int vsprintf(char *, const char *, va_list);

○ The buffer size provided to the method may be incorrect.

◉ The function will write past the end of the buffer.

○ When used inside a loop, a programmer may forget to consider the buffer size.

> View Feedback

Question 9   1 / 1 point

A programmer purposely and obfuscatedly inserts malicious code so she may later alter the execution of a program to her advantage. This is an example of a:

○ Virus

◉ Trapdoor

○ Salami Attack

○ Trojan Horse

○ Covert Channel

> View Feedback

Question 10   1 / 1 point

A large music company decides to aggresively end pirating of its music by secretly compromising the security of everyone's computers when they attempt to play a compact disc they legitimately bought. This is an example of a:

○ Virus

○ Trapdoor

○ Salami Attack

◉ Trojan Horse

○ Covert Channel

> View Feedback

Question 11   1 / 1 point

How can somebody check whether her program does something which it should not do?

○ Using exhaustive testing

○ Including unexpected behaviour as 'Don't's in her design specification

◉ Doing program verification using formal methods

> View Feedback

Attempt Score: 11 / 1

Overall Grade (last attempt)**:** 11 / 1

○ Using exhaustive testing

○ Including unexpected behaviour as 'Don't's in her design specification