ASSESSMENT

TOPIC: BUFFER OVERFLOW

1. What typically happens when a buffer is overflowed

A. The memory space that comes after the buffer holds the extra data as well as keeping the data that it contained before.
B. Whatever is in the memory space that comes after the buffer is overwritten. *
C. The memory chip in the computer gets too big and explodes.
D. Electrons fall out of the chip and start a fire.
E. Both A and B

2.What can make a buffer overflow a security problem?

A. Only when the attacker is able to hijack the execution of the program
B. Only when the buffer overflow is between two computers on a network.
C. When sensitive data is over written
D. When data that is critical to the execution of the program is overwritten causing the program to crash.
E. Both C and D*

3.What can happen if a buffer overflow causes a program to crash?

A. A core dump gives the attacker access to confidential data
B. A denial of service attack where other users on the network can no longer access the service
C. The computer can catch on fire.
D. Nothing bad can happen unless the attacker is able to hijack the machine or overwrite confidential data.
E. Both A and B*

4.Which of these kinds of inputs can cause buffer overflow?

A. A floating point numbers
B. A single integer
C. Strings
D. An environmental variable
E. File input
F. All of the Above *

5.How many types of buffer overflows are there?

A. 1
B. 2*
C. 3
D. 4
E. 5

6.Applications developed by programming languages like _____ and _____ prone to buffer overflow error.

A. C, Ruby
B. Python, Ruby
C. C, C++ *
D. TCL, C++

WHAT TO SUBMIT

Submit the document by answering all the questions.