Krutarth Panchal

CIS 450

Week 6 - Stack Based Windows Buffer Overflow

1. What is a buffer overflow attack?

According to OWASP buffer overflow attack is overwriting the memory fragments of the process, which should have never been modified intentionally or unintentionally. In other words, a buffer overflow attacks is occurs when a program is force to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.

1. What is the purpose of a debugger?

The purpose of the debugger to see the inner workings of the program at the time of the crash once the buffer overflow occurs. It also provides the information about the crash which can be used to structure a buffer to be sent to the application.

1. Why would one control an extended instruction pointer (EIP)?

EIP is the instruction pointer, which is a register, it points to the next command. The computer CPU decides the instruction to executing next by reading the value of the EIP register and performing the instructions found at that memory address. By controlling the EIP we can have the program execute the command send to another location of the memory or simply crashing the program which block other user to have access to the program.

1. What OS is especially vulnerable to EIP?

Windows XP SP2 is especially vulnerable to EIP.

1. It's impossible to patch against buffer overflow exploits. (T or F)

True

1. What kinds of attacks can buffer overflow be used to create?

Stack-based buffer overflows and Heap-based attacks are the kinds of attacks buffer overflow can be used to create.

1. Hackers do not test (proof of concept) their exploits. (T or F)

False

1. Msfvenom cannot be used to carry out code execution and shellcode. (T or F

False