Week 10 and 11 Let’s Crash and Callback  
CIS 450  
Krutarth Panchal

### Overwrite SEH and ASLR Questions (Book)

Answer the following questions from the book.

1. What is SEH?  
   SEH (Structured Exception Handling) is a Microsoft extension for C/C++ to manage exceptions like hardware faults.
2. How does SEH work?  
   SEH relies on a stack unwinding mechanism to handle exceptions. When an error occurs, it searches for a handler function defined in a try-except block.
3. How can SEH be exploited?  
   SEH vulnerabilities can be exploited by attackers to overwrite control flow. By crafting malicious code, they can redirect program execution for unintended purposes.
4. What is ASLR?  
   ASLR (Address Space Layout Randomization) is a security feature that randomizes the base addresses for key parts of a program's memory layout (e.g., code, heap, stack).
5. How does ASLR work?  
   ASLR makes it harder for attackers to predict memory locations for exploitation attempts. They can't directly target specific addresses for code injection.
6. How can ASLR be exploited?  
   While ASLR thwarts some exploits, advanced techniques can bypass it. Information leakage from the program or brute-forcing memory addresses are potential methods.
7. What are two Linux Kernel/Stack or Heap vulnerabilities reported (from 2018 until now)?  
   One is CVE-2018-17182. The flaw can also be exploited to achieve arbitrary code execution as root and affects all kernel versions since 3.16. Another was CVE-2018-14634. The flaw is located in Linux kernel’s create\_elf\_tables() function and can be exploited on 64-bit systems by local users with access to SUID binaries.
8. What were they designed to do?  
   Kernel/Stack/Heap vulnerabilities are designed to crash the system, gain unauthorized access, or elevate privileges.
9. Exploiting the EIP doesn't work for Windows or Linux Stack smashing or compromise. (T or F)  
   False. Exploiting the EIP (Instruction Pointer) is a common technique in both Windows and Linux stack smashing to redirect program execution and achieve unauthorized control.
10. What are two Windows Kernel/Stack vulnerabilities reported in 2019/2020?  
    a. CVE-2020-17087  
    b. CVE-2019-1472 and CVE-2019-1474