Computer Security: Principles and Practice, 2nd Edition Chapter 10

**Chapter 10 – Buffer Overflow**

1. A buffer overrun is a condition where more input is placed into a buffer or data holding area than the capacity allocated and thus overwrites other information.

1. At the basic machine level, all of the data manipulated by machine instructions executed by the computer processor are stored in either the processor’s registers or in memory.

1. Unix was one of the earliest operating systems written in a high-level language.

1. A stack buffer overflow occurs when the targeted buffer is located on the stack, usually as a local variable in a function’s stack frame.

1. The function of the shellcode was to transfer control to a user command line interpreter that gave access to any program available on the system with the privileges of the attacked program.

1. One of the restrictions on the content of shellcode is that it has to be position independant, which means that it cannot contain any absolute address referring to itself.

1. Compile-time defenses aim to harden programs to resist attacks in new programs.

1. Run-time defenses aim to detect and abort attacking existing programs.

1. The OpenBSD project produces a free, multiplatform 4.4BSD-based UNIX-like operating system.

1. Stackshield, Return Address Defender and Stackguard are GCC compiler extensions that insert additional function entry and exit code.

1. Off-by-one attacks can occur in a binary buffer copy when the programmer has included code to check the number of bytes being transferred, but due to a coding error, allows just one more byte to be copied than there is space available.

1. In 1996 Aleph One published “Smashing the Stack for Fun and Profit” in *Phrack* magazine, giving a step-by-step introduction to exploiting stack-based buffer overflow vulnerabilities.

1. A buffer overflow can occur as a result of a programming error when a process attempts to store data beyond the limits of a fixed-sized buffer and consequently overwrites adjacent memory locations.

Computer Security: Principles and Practice, 2nd Edition Chapter 10

1. Guard pages can be placed between stack frames or between different allocations on the heap to provide further protection against stack and heap overflow attacks, but at cost in execution time supporting the large number of page mappings necessary.

1. The attacker can specify the return address used to enter code as a location somewhere in the run of NOPs, which is called a NOP sled.