**Chapter 10 – Buffer Overflow**

**TRUE/FALSE QUESTIONS:**

T F 1. Buffer overflow attacks are one of the most common attacks seen.

T F 2. Buffer overflow exploits are no longer a major source of concern to

security practitioners.

T F 3. A buffer overflow error is not likely to lead to eventual program

termination.

T F 4. To exploit any type of buffer overflow the attacker needs to identify a

buffer overflow vulnerability in some program that can be triggered

using externally sourced data under the attackers control.

T F 5. 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.

T F 6. Even though it is a high-level programming language, Java still suffers

from buffer overflows because it permits more data to be saved into a buffer than it has space for.

T F 7. Stack buffer overflow attacks were first seen in the Aleph One Worm.

T F 8. A stack overflow can result in some form of a denial-of-service attack

on a system.

T F 9. An attacker is more interested in transferring control to a location and

code of the attacker’s choosing rather than immediately crashing the

program.

T F 10. The potential for a buffer overflow exists anywhere that data is copied

or merged into a buffer, where at least some of the data are read from

outside the program.

T F 11. Shellcode is not specific to a particular processor architecture.

T F 12. There are several generic restrictions on the content of shellcode.

T F 13. An attacker can generally determine in advance exactly where the

targeted buffer will be located in the stack frame of the function in

which it is defined.

T F 14. Shellcode must be able to run no matter where in memory it is

located.

T F 15. Buffer overflows can be found in a wide variety of programs,

processing a range of different input, and with a variety of possible

responses.

**MULTIPLE CHOICE QUESTIONS:**

1. The buffer overflow type of attack has been known since it was first widely used by the \_\_\_\_\_\_\_\_\_\_ Worm in 1988.

A. Code Red B. Slammer

C. Morris Internet D. Alpha One

1. A buffer \_\_\_\_\_\_\_\_\_ is a condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information.

A. overflow B. overrun

C. overwrite D. all the above

1. A consequence of a buffer overflow error is \_\_\_\_\_\_\_\_\_\_ .
2. corruption of data used by the program
3. unexpected transfer of control in the program
4. possible memory access violation
5. all the above
6. A stack buffer overflow is also referred to as \_\_\_\_\_\_\_\_\_\_\_ .

A. stack framing B. stack smashing

C. stack shocking D. stack running

1. The function of \_\_\_\_\_\_\_\_ was to transfer control to a user command-line interpreter, which gave access to any program available on the system with the privileges of the attacked program.

A. shellcode B. stacking

C. no-execute D. memory management

1. The Packet Storm Web site includes a large collection of packaged shellcode, including code that can:
2. create a reverse shell that connects back to the hacker
3. flush firewall rules that currently block other attacks
4. set up a listening service to launch a remote shell when connected to
5. all the above
6. \_\_\_\_\_\_\_\_\_\_ aim to prevent or detect buffer overflows by instrumenting programs when they are compiled.

A. Compile-time defenses B. Shellcodes

C. Run-time defenses D. All the above

1. \_\_\_\_\_\_\_\_\_\_ can prevent buffer overflow attacks, typically of global data, which

attempt to overwrite adjacent regions in the processes address space, such as the global offset table.

A. MMUs B. Guard pages

C. Heaps D. All the above

1. \_\_\_\_\_\_\_\_\_ is a form of overflow attack.

A. Heap overflows B. Return to system call

C. Replacement stack frame D. All the above

1. The \_\_\_\_\_\_\_\_\_\_ used a buffer overflow exploit in “fingerd” as one of its attack

mechanisms.

A. Code Red Worm B. Sasser Worm

C. Morris Internet Worm D. Slammer Worm

1. In 2003 the \_\_\_\_\_\_\_\_\_ exploited a buffer overflow in Microsoft SQL Server 2000.

A. Slammer worm B. Morris Internet Worm

C. Sasser worm D. Code Red worm

1. A buffer overflow in MicroSoft Windows 2000/XP Local Security Authority Subsystem Service was exploited by the \_\_\_\_\_\_\_\_\_ .

A. Aleph One B. Sasser worm

C. Slammer worm D. none of the above

13. The buffer is located \_\_\_\_\_\_\_\_\_\_ .

A. in the heap B. on the stack

C. in the data section of the process D. all the above

1. \_\_\_\_\_\_\_\_\_ is a tool used to automatically identify potentially vulnerable programs.

A. Slamming B. Sledding

C. Fuzzing D. All the above

1. Traditionally the function of \_\_\_\_\_\_\_\_\_\_ was to transfer control to a user command-line interpreter, which gave access to any program available on the system with the privileges of the attacked program.

A. shellcode B. C coding

C. assembly language D. all the above

**SHORT ANSWER QUESTIONS:**

1. A \_\_\_\_\_\_\_\_\_\_ can occur as a result of a programming error when a process attempts to store data beyond the limits of a fixed-size buffer and consequently overwrites adjacent memory locations.
2. Data is simply an array of \_\_\_\_\_\_\_\_\_ .
3. A \_\_\_\_\_\_\_\_\_\_\_ overflow occurs when the targeted buffer is located on the stack, usually as a local variable in a function’s stack frame.
4. “Smashing the Stack for Fun and Profit” was a step by step introduction to exploiting stack-based buffer overflow vulnerabilities that was published in *Phrack* magazine by \_\_\_\_\_\_\_\_\_ .
5. An essential component of many buffer overflow attacks is the transfer of execution to code supplied by the attacker and often saved in the buffer being overflowed. This code is known as \_\_\_\_\_\_\_\_\_ .
6. Shellcode has to be \_\_\_\_\_\_\_\_\_\_, which means it cannot contain any absolute address referring to itself.
7. \_\_\_\_\_\_\_\_\_\_ defenses aim to harden programs to resist attacks in new programs.
8. \_\_\_\_\_\_\_\_\_\_ defenses aim to detect and abort attacks in existing programs.
9. The \_\_\_\_\_\_\_\_\_\_ project produces a free, multiplatform 4.4BSD-based UNIX-like operating system.
10. \_\_\_\_\_\_\_\_\_\_ is one of the best known protection mechanisms that is a GCC compiler extension that inserts additional function entry and exit code.
11. A \_\_\_\_\_\_\_\_\_ value is named after the miner’s bird used to detect poisonous air in a mine and warn miners in time for them to escape.
12. \_\_\_\_\_\_\_\_\_ 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.
13. The \_\_\_\_\_\_\_\_\_ is typically located above the program code and global data and grows up in memory (while the sack grows down toward it).
14. Gaps, or \_\_\_\_\_\_\_\_\_\_ , are flagged in the MMU as illegal addresses, and any attempt to access them results in the process being aborted.
15. In the classic \_\_\_\_\_\_\_\_\_\_ overflow, the attacker overwrites a buffer located in the local variable area of a stack frame and then overwrites the saved frame pointer and return address.