

BUFFER OVERFLOW SCAVENGER HUNT

Susan Gerhart, gerharts@erau.edu

Embry-Riddle Aeronautical University • Prescott, Arizona • USA

This Document was Funded by the National Science Foundation Federal Cyber Service Scholarship For Service Program:
Grant No. 0113627

©2002, Susan Gerhart, Jedidiah R. Crandall, Jan G. Hogle. <http://nsfsecurity.pr.erau.edu>.
Distributed July 2002.

Find:

1. The name and author of a book published by Microsoft press that refers to the buffer overflow problem as "Public Enemy #1" (Easy)
2. A major software vendor that has not released a single buffer overflow (Difficult)
3. A major operating system for which fewer than 10 buffer overflow security alerts were released within a full year (Difficult)
4. A software engineering, programming languages, operating systems, or C programming college textbook that gives a good explanation of buffer overflows and how to prevent them (Difficult)
5. A software engineering, programming languages, operating systems, or C programming college textbook with a stupid cartoon in it (Easy)
6. A network security book that does not have buffer overflow in its index (Easy)
7. A buffer overflow security alert currently posted on a security news website (Easy)
8. An instance where a buffer overflow led to a cost not associated with the cost of fixing and cleaning up after the buffer overflow (Who knows?)
9. A checklist (other than ours) for programmers and testers that is intended to prevent buffer overflows (Difficult)
10. A paper published in 1996 that dramatically increased the number of buffer overflow attacks the their sophistication. (Moderate)

11. The year in which security alerts will exceed 50,000 at the current annual rate of growth. (Easy)
12. A script that uses a buffer overflow exploit to gain root access on your favorite flavor of UNIX (Easy)
13. A statement by a software vendor that they will not release any more buffer overflows (Easy)
14. A statement by a software vendor that they will not release any more buffer overflows that was not proven false by the discovery of a buffer overflow in their newest software soon after (Difficult)
15. A statement by a well-known politician that gives some indication that they knew what the Y2K problem was (Easy)
16. A statement by a well-known politician that gives some indication that they know what a buffer overflow is (Difficult)
17. A statement from a book publisher about a book that refers to buffer overflows as "the most wicked of attacks" (Easy)
18. A definition of Trustworthy Computing in Microsoft-speak.
19. Other definitions of Trustworthy and Trusted Computing.
20. An explanation of why Microsoft refers to "buffer overruns" when the rest of the world says "buffer overflows". (Who knows?)

This document is part of a larger package of materials on buffer overflow vulnerabilities, defenses, and software practices. For more information, go to: <http://nsfsecurity.pr.erau.edu>

Also available are:

- Demonstrations of how buffer overflows occur (Java applets)
- PowerPoint lecture-style presentations on an introduction to buffer overflows, preventing buffer overflows (for C programmers), and a case study of Code Red
- Checklists and Points to Remember for C Programmers
- An interactive module and quiz set with alternative paths for journalists/analysts and IT managers as well as programmers and testers
- A scavenger hunt on implications of the buffer overflow vulnerability

Please complete a feedback form at <http://nsfsecurity.pr.erau.edu/feedback.html> to tell us how you used this material and to offer suggestions for improvements.