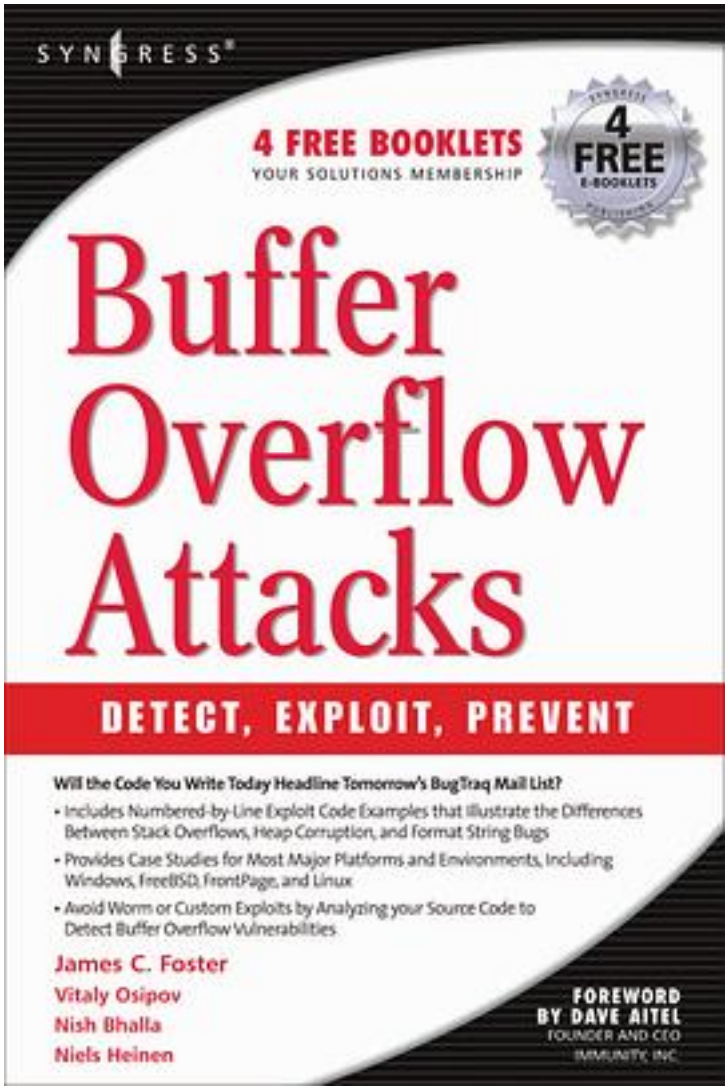
Buffer Overflow Attacks



Buffer Overflow Attacks_下载链接1_

著者:Foster, James C. (EDT)

出版者:Elsevier Science Ltd

出版时间:

装帧:Pap

isbn:9781932266672

The SANS Institute maintains a list of the “Top 10 Software Vulnerabilities.” At the current time, over half of these vulnerabilities are exploitable by Buffer Overflow attacks, making this class of attack one of the most common and most dangerous weapon used by malicious attackers. This is the first book specifically aimed at detecting, exploiting, and preventing the most common and dangerous attacks.

Buffer overflows make up one of the largest collections of vulnerabilities in existence; And a large percentage of possible remote exploits are of the overflow variety. Almost all of the most devastating computer attacks to hit the Internet in recent years including SQL Slammer, Blaster, and I Love You attacks. If executed properly, an overflow vulnerability will allow an attacker to run arbitrary code on the victim’s machine with the equivalent rights of whichever process was overflowed. This is often used to provide a remote shell onto the victim machine, which can be used for further exploitation.

A buffer overflow is an unexpected behavior that exists in certain programming languages. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker’s perspective and defending against these attacks for the software developer.

*Over half of the “SANS TOP 10 Software Vulnerabilities” are related to buffer overflows.

*None of the current-best selling software security books focus exclusively on buffer overflows.

*This book provides specific, real code examples on exploiting buffer

overflow attacks from a hacker’s perspective and defending against these attacks for the software developer.

作者介绍:

目录:

Buffer Overflow Attacks_下载链接1_

标签

安全

programming

Assembly

编程

安全技术

评论

真是一本好书!

图书馆书籍

Buffer Overflow Attacks_下载链接1_

书评

Buffer Overflow Attacks_下载链接1_