1. Record Nr. UNISALENTO991003260139707536

Titolo	Buffer overflow attacks [electronic resource] : detect, exploit, prevent / James C. Foster ... [et al.] ; foreword by Dave Aitel
Pubbl/distr/stampa	Rockland, MA : Syngress, c2005
ISBN	9781932266672 1932266674
Descrizione fisica	xxii, 497 p. : ill. ; 23 cm.
Altri autori (Persone)	Foster, James C.
Disciplina	005.8
Soggetti	Computer security Computer viruses Electronic books.
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Buffers and overflows ; Stack segment ; Attacks on the stack ; Attacks on the heap ; Discovering vulnerabilities ; Crafting a payload ; Attack delivery ; Real world examples ; Trapping attacks ; Preventing attacks ; Defense in depth.
Sommario/riassunto	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 victims 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.