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.

2.

Record Nr.	UNINA9910720694803321
Autore	Canfora, Luciano
Titolo	Il passato presente / Luciano Canfora ; a cura di Chiara Bozzoli
Pubbl/distr/stampa	Roma, : Teti, 2022
ISBN	978-88-314-9256-0
Descrizione fisica	120 p. ; 21 cm
Collana	Historos
Disciplina	858.92
Locazione	FLFBC
Collocazione	907.2 CANL 05
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	«La storia si scrive sempre usando il tempo presente». Come si definisce oggi un maitre à penser? Se consideriamo tale chi è in grado di dare significato a ciò che accade tracciando una rete di relazioni tra passato e presente, mettendo il proprio sapere specialistico al servizio dell'attualità, Luciano Canfora lo è certamente. Gli strumenti della filologia, lo sguardo limpido, scevro da partigianerie e conformismi, diventano in questa raccolta di saggi efficaci dispositivi per indagare i grandi temi del pensiero contemporaneo. Antidogmatico per eccellenza e per formazione, sempre capace di esplorare prospettive multidisciplinari e di individuare continuità nel mutamento incessante della storia, Luciano Canfora ci offre una chiave di lettura per affrontare le sfide del presente.

3. Record Nr. UNINA9910263946703321

Titolo	Material religion : the journal of objects, art and belief
Pubbl/distr/stampa	Oxford, Eng. : , : Berg, , 2005-
ISSN	1751-8342
Soggetti	Art and religion Religion Religious articles Art et religion Objets religieux religion (discipline) religious objects Ritus Sachkultur Godsdienst Materiële cultuur Religieuze symboliek Periodicals.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Periodico
Note generali	Refereed/Peer-reviewed