1. Record Nr. UNISA996465522703316

Titolo	Recent Advances in Intrusion Detection [[electronic resource]] : 10th International Symposium, RAID 2007, Gold Coast, Australia, September 5-7, 2007, Proceedings / / edited by Christopher Kruegel, Richard Lippmann, Andrew Clark
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-74320-0
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XII, 340 p.)
Collana	Security and Cryptology ; ; 4637
Disciplina	005.8
Soggetti	Data encryption (Computer science) Management information systems Computer science Computers and civilization Computer communication systems Operating systems (Computers) Cryptology Management of Computing and Information Systems Computers and Society Computer Communication Networks Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"... the 10th Symposium on Recent Advances in Intrusion Detection (RAID 2007)"--Pref.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Host-Based Intrusion Detection -- Exploiting Execution Context for the Detection of Anomalous System Calls -- Understanding Precision in Host Based Intrusion Detection -- Anomaly-Based Intrusion Detection -- Comparing Anomaly Detection Techniques for HTTP -- Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications -- Network-Based Intrusion Detection and Response -- Emulation-Based Detection of Non-self-contained Polymorphic Shellcode -- The NIDS Cluster: Scalable, Stateful Network Intrusion Detection on Commodity Hardware -- Cost-Sensitive Intrusion

Responses for Mobile Ad Hoc Networks -- Insider Detection and Alert Correlation -- elicit: A System for Detecting Insiders Who Violate Need-to-Know -- On the Use of Different Statistical Tests for Alert Correlation – Short Paper -- Malicious Code Analysis -- Automated Classification and Analysis of Internet Malware -- “Out-of-the-Box” Monitoring of VM-Based High-Interaction Honeypots -- A Forced Sampled Execution Approach to Kernel Rootkit Identification -- Evasion -- Advanced Allergy Attacks: Does a Corpus Really Help? -- Alert Verification Evasion Through Server Response Forging -- Malicious Code Defense -- Hit-List Worm Detection and Bot Identification in Large Networks Using Protocol Graphs -- SpyShield: Preserving Privacy from Spy Add-Ons -- Vortex: Enabling Cooperative Selective Wormholing for Network Security Systems.