

1. Record Nr.	UNINA9910484233803321
Titolo	Recent advances in intrusion detection : 10th International Symposium, RAID 2007, Gold Coast [i.e. Coast], Australia, September 5-7, 2007 : proceedings / / Christopher Kruegel, Richard Lippmann, Andrew Clark (eds.)
Pubbl/distr/stampa	Berlin, : Springer-Verlag, c2007
ISBN	3-540-74320-0
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XII, 340 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 4637 LNCS sublibrary. SL 4, Security and cryptology
Altri autori (Persone)	KruegelChristopher <1976-> LippmannRichard ClarkAndrew <1971->
Disciplina	005.8
Soggetti	Computer security Computers - Access control
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.
