1. Record Nr.	UNINA9910143895503321
Titolo	Recent Advances in Intrusion Detection : 5th International Symposium, RAID 2002, Zurich, Switzerland, October 16-18, 2002, Proceedings / / edited by Andreas Wespi, Giovanni Vigna, Luca Deri
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-36084-0
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (X, 327 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2516
Disciplina	005.8
Soggetti	System safety Computer science Computer networks Operating systems (Computers) Data encryption (Computer science) Computers and civilization Security Science and Technology Computer Science, general Computer Communication Networks Operating Systems Cryptology Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Stepping Stone Detection -- Detecting Long Connection Chains of Interactive Terminal Sessions -- Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay -- Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses -- Anomaly Detection -- Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits -- Correlation -- Analyzing Intensive Intrusion Alerts via Correlation -- A Mission-Impact-Based Approach to INFOSEC Alarm Correlation -- M2D2: A Formal Data Model for IDS Alert Correlation --

Sommario/riassunto

On behalf of the program committee, it is our pleasure to present to you the proceedings of the Fifth Symposium on Recent Advances in Intrusion Detection (RAID). Since its ?rst edition in 1998, RAID has established itself as the main annual intrusion detection event, attracting researchers, practitioners, and v- dors from all over the world. The RAID 2002 program committee received 81 submissions (64 full papers and 17 extended abstracts) from 20 countries. This is about 50% more than last year. All submissions were carefully reviewed by at least three program comm- tee members or additional intrusion-detection experts according to the criteria ofscienti?cnovelty, importancetothe?eld,andtechnicalquality.Finalselection took place at a meeting held on May 15–16, 2002, in Oakland, USA. Sixteen full papers were selected for presentation and publication in the conference procdings. In addition, three extended abstracts of work in progress were selected for presentation. The program included both fundamental research and practical issues. The seven sessions were devoted to the following topics: anomaly detection, steppi- stonedetection, correlationofintrusion-detectionalarms,assessmentofintrusi-detectionsystems,intrusiontolerance,legalaspects,adaptiveintrusion-detection systems, and intrusion-detection analysis. RAID 2002 also hosted a panel on “Cybercrime,” a topic of major concern for both security experts and the public. Marcus J. Ranum, the founder of Network Flight Recorder, Inc., delivered a keynote speech entitled “Challenges for the Future of Intrusion Detection”.