CIDS: An agent-based intrusion detection system

D. Dasgupta*, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsetti

Intelligent Security Systems Research Laboratory, Division of Computer Science, The University of Memphis, Memphis, TN 38152, United States

Received 1 July 2003; revised 6 October 2004; accepted 21 January 2005

KEYWORDS
Security agents; Cougaar; Plugin; Intrusion detection; Decision support

Abstract The paper describes security agent architecture, called CIDS, which is useful as an administrative tool for intrusion detection. Specifically, it is an agent-based monitoring and detection system, which is developed to detect malfunctions, faults, abnormalities, misuse, deviations, intrusions, and provide recommendations (in the form of common intrusion detection language). The CIDS can simultaneously monitor networked-computer activities at multiple levels (user to packet level) in order to find correlation among the deviated values (from the normal or defined policy) to determine specific security violations. The current version of CIDS (CIDS 1.4) is tested with different simulated attacks in an isolated network, and some of those results are reported here.
© 2005 Elsevier Ltd. All rights reserved.

Introduction

With the growing use of Internet applications and automated scripts, it has become very difficult to keep track of all cyber activities. While it is hard to track each and every application, in particular most exploitable ones such as Active scripting (JScript, VBScript), ActiveX, Outlook, Outlook Express, etc. it is possible to monitor their effects on the system and its resources. Moreover, it is necessary to efficiently analyze monitored network data for faster attack detection and response.

Intrusion/anomaly detection (Anderson, 1980; Axelsson et al., 1996; Denning, 1987; Dunlap and Dasgupta, 2002; Krügel and Toth, 2001; Roesch, 1999; Chari and Cheng, 2003) is an important part of network security. There are many intrusion detection systems (IDS) commercially available. A detailed survey and taxonomy of practical IDSs may be found in the literature (Allen et al., 2000; Debar et al., 1999). Some are anomaly based and others are signature based. Security researchers also formed working groups to develop common framework, methodology and description language for intrusion detection systems (Lee and Stolfo, 2000;