Chapter 24
The Conceptual and Architectural Design of an Intelligent Intrusion Detection System

Mradul Dhakar
ITM University Gwalior, India

Akhilesh Tiwari
Madhav Institute of Technology and Science, India

ABSTRACT

The tremendous work in the field of security has made enormous efforts towards the ascertainment of innovative ideas along with their practical applicability. These motivated the security agencies to adopt them practically. But adequate remedies are not accomplished yet due to the enhanced technological aspects even in the unlawful communities. These communities have become a major concern for the security agencies and can be considered as unaddressed issue. This concern led to the introduction of Intrusion Detection Systems (IDSs). The IDS is a means for detecting the intrusive events concealed among the activities of normal users. Additionally, such systems also provide necessary assistance in preventing future intrusions. The present chapter focuses on improving the performance of the IDS in order to meet the contemporary progression by proposing a system that is able to achieve a system that is effective, adaptive and intelligent in nature and is able to remarkably detect intrusions. In order to accomplish the desired system, the chapter involves development of intelligent IDS.

INTRODUCTION

Now-a-days, revolution of the internet has made it possible to connect all the corners of the world and empowers the user to share data in an easy and fastest manner. Although this is a convenient mode of communication but it requires much of data to be stored on the web with the necessity of being secured. The increased number of adverse attacks on web resources has called forth the security concerns. This

DOI: 10.4018/978-1-5225-9866-4.ch024

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

led to the successful implementation of a system capable of detecting abnormalities (generally referred as intrusions). This detection system is recognized as Intrusion Detection System (IDS).

The process of surveillance of the user's network activities and then identifying and distinguishing the normal and abnormal activities is termed as intrusion detection whereas the dedicated system used for intrusion detection is known as Intrusion Detection System (IDS). Whenever an intruder attempts to compromise the availability, integrity or confidentiality of the system or the whole network itself, the IDS monitors and identifies the prohibited activities and forbids the illicit users from accessing services or resources of the computer system or the network. The system performs the relevant actions by taking various predefined anticipations into consideration.

Intrusion Detection System (Mohammad, Sulaiman & Muhsin, 2011; Parekh, Madan & Tugnayat, 2012) is basically software or the combination of software and hardware that automates the process of tracking and analyzing of events on the web. The IDS has the capability to detect the intrusion in network by being in charge of taking action against any intrusion sensed. It generates an alarm whenever any intrusion is detected in the traffic. But sometimes there are the cases when a user is accidently detected as intruder as much of his/her activities match the abnormal behavior and as a result generates the alarm. This type of generation of alarm is named as a false alarm.

In order to decrease the rate of false alarm IDS was amalgamated with various Artificial Intelligence (AI) techniques. Despite of available promising AI techniques such as rule based expert system, genetic algorithm, inductive sequential patterns, state transition analysis and artificial neural network in IDS; the IDS is still facing problems in effective pattern recognition and classification. Data mining with its techniques in this context have proved itself as the most prominent way for handling these problems.

The key ideas are to use data mining techniques to discover consistent and useful patterns of system features that describe the program and user behavior, and use the set of relevant system features to compute (inductively learned) classifiers that can recognize anomalies and known intrusions (Lee & Stolfo, 1998). With this thought, data mining based IDS has come out as the frequently preferred approach.

When applying data mining technology to intrusion detection systems, it can mine the features of new and unknown attacks well, which is a maximal help to the dynamic defense of intrusion detection system (Song & Ma, 2009). Data mining based IDS has the advantage of potentially being able to detect new attacks and prevent the attack on a network (Raut & Gawali, 2012). This enables the system to cope up with the advancements. Furthermore, use of data mining techniques for intrusion detection helps in identifying the trends within data that go beyond simple analysis (Feruza & Yusufovna, 2008).

In order to provide greater security policies, IDS is classified into Misuse and Anomaly Detection categories, discussed in further section.

TYPES OF ATTACK

This Section describes the major types of attack that are being detected by an intrusion detection system. There are four major attack categories (Peddabachigari, Abraham, Grosanc & Thomas, 2007; Jiang, Song, Wang, Han & Li, 2006) in general and are described in the following subsections.

- **Denials-of-Service (dos):** Denial of Service is the type of attack where the legitimate users are restrained from accessing the services of a host or network resources. The attacker makes the re-

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/the-conceptual-and-architectural-design-of-an-intelligent-intrusion-detection-system/234958

Related Content

Content-Aware Caching for Cooperative Transcoding Proxies
Kyungbaek Kim, Byungjip Kimand Daeyeon Park (2008). *Encyclopedia of Internet Technologies and Applications (pp. 112-118).*
www.irma-international.org/chapter/content-aware-caching-cooperative-transcoding/16842

Actors in the Emerging Internet of Things Ecosystems
Seppo Leminen, Mervi Rajahonkaand Mika Westerlund (2020). *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 1587-1607).*
www.irma-international.org/chapter/actors-in-the-emerging-internet-of-things-ecosystems/235009

Clustering in Wireless Sensor Networks: Context-Aware Approaches
Enamul Haqueand Norihiko Yoshida (2012). *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications (pp. 197-211).*
www.irma-international.org/chapter/clustering-wireless-sensor-networks/63551

Converging Technologies for the IoT: Standardization Activities and Frameworks
Dragorad Milovanovi, Vladan Pantoviand Gordana Gardaševi (2020). *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 1070-1095).*
www.irma-international.org/chapter/converging-technologies-for-the-iot/234983

Transporting TDM Service on Metropolitan Bus-Based Optical Packet Switching Networks
Viet Hung Nguyenand Tülin Atmaca (2008). *Encyclopedia of Internet Technologies and Applications (pp. 653-662).*
www.irma-international.org/chapter/transporting-tdm-service-metropolitan-bus/16917