Computers and Electrical Engineering 35 (2009) 517–526

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A hybrid intrusion detection system design for computer network security

M. Ali Aydın *, A. Halim Zaim, K. Gökhan Ceylan

Department of Computer Engineering, Faculty of Engineering, Istanbul University, 34320 Avcilar, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 14 March 2007
Received in revised form 15 July 2008
Accepted 30 December 2008
Available online 8 February 2009

Keywords:
Computer networks
Computer network security
Intrusion detection systems
Hybrid intrusion detection system

ABSTRACT

Intrusions detection systems (IDSs) are systems that try to detect attacks as they occur or after the attacks took place. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. Intrusion detection systems can be misuse-detection or anomaly detection based. Misuse-detection based IDSs can only detect known attacks whereas anomaly detection based IDSs can also detect new attacks by using heuristic methods. In this paper we propose a hybrid IDS by combining the two approaches in one system. The hybrid IDS is obtained by combining packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project.

The hybrid IDS obtained is evaluated using the MIT Lincoln Laboratories network traffic data (IDEVAL) as a testbed. Evaluation compares the number of attacks detected by misuse-based IDS on its own, with the hybrid IDS obtained combining anomaly-based and misuse-based IDSs and shows that the hybrid IDS is a more powerful system.

1. Introduction

Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users.

Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them.

It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusions detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems so that they are not repeated [1].

IDSs collect information from a computer or a computer network in order to detect attacks and misuses of the system. Many IDSs only analyze the attacks and some of them try stopping the attack at the time of the intrusion. Three types of data are used by IDSs. These are network traffic data, system level test data and system status files [2,3].

In "2003CSI/FBI Computer Crime and Security Survey" it has been stated that the IDS usage in 1999 had been 42% and this ratio has become 73% in year 2003. This great improvement shows that IDSs are very important as security technologies. This paper is organized as follows: intrusion detection systems are described in Section 2, IDS types are explained in Section 3: Snort is the chosen system as misuse-based IDS; PHAD and NETAD are chosen as anomaly-based IDSs. Section 4 gives a brief

* Corresponding author. Tel.: +90 2124737070x17544; fax: +90 2124737044.
E-mail addresses: aydinali@istanbul.edu.tr (M.A. Aydın), ahzaim@istanbul.edu.tr (A.H. Zaim), kgceylan@istanbul.edu.tr (K.G. Ceylan).

0045-7906/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2008.12.005

description of the hybrid IDS we propose in this paper. The newly obtained hybrid IDS is evaluated in Section 5 and finally Section 6 includes conclusion.

2. Intrusion detection systems

Intrusion detection systems are hardware and software systems that monitor events occurred on computers and computer networks in order to analyze security problems. The number and severity of these attacks has been increasing continuously. Consequently IDSs have become an integral part of the security infrastructure of organizations.

Intrusions to computer networks are called as "attacks" and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms. Attacks can be originated from users who login to the computer using the Internet trying to gain *superuser* or *administrator* rights and other users who misuse the rights they have. IDSs automate monitoring and analyzing the attacks [1,2,4].

3. IDS types

There are two approaches to analyzing of events using IDSs. These are misuse-based and anomaly-based approaches. Misuse-based IDSs aim to distinguish events that violate system policy. Anomaly-based IDSs try analyzing abnormal activities and flag these activities as attacks. Both approaches have advantages and disadvantages when compared to each other [1,2,5].

Snort is the most commonly used signature-based intrusion detection system. Snort is a network intrusion detection system that runs over IP networks analyzing real-time traffic for detection of misuses [6]. Snort depends on a template-matching scheme and makes content analysis. It has the ability to flag alerts depending on pre-defined misuse rules and saves packets in tcpdump files or in plain text files. Snort is preferred to be used in academic research projects as it is an open-source tool and for this reason we have also chosen Snort as the signature-based intrusion detection system in our work.

Anomaly detection based intrusion detection systems are separated into many sub-categories in the literature including statistical methodologies [7–10], data mining [11,12], artificial neural networks [13], genetic algorithms [14] and immune systems [15,16]. Among these sub-categories, statistical methods are the most commonly used ones in order to detect intrusions by analyzing abnormal activities occurring in the network. PHAD [17] and NETAD [18] statistical methods are chosen as the anomaly-based intrusion detection systems in this paper. We have implemented a hybrid IDS by mounting anomaly-based IDSs PHAD and NETAD to Snort as a preprocessor. PHAD is different than the other conventional network-based anomaly detection systems for two reasons. First, it models protocols rather than user behaviors. Second, it uses a time-based model depending on the rapid change of network statistics in short term. PHAD flags only the first anomaly it detected as an alert even if there is a series of the same anomaly recurring. This feature of PHAD helps reducing the number of false alerts. NETAD, models single packets like PHAD, uses dynamic-conditioned rules like ALAD [19], and rule verification like LERAD [20]. Its greatest contribution is modeling values that are not new.

3.1. Misuse-based IDSs

Misuse detectors analyze system activities and try to find a match between these activities and known attacks having definitions or signatures introduced to the system beforehand [1,2,21].

Advantages:

- Misuse detectors are very efficient in detecting attacks without signaling false alarms (FA).
- Misuse detectors can quickly detect specially designed intrusion tools and techniques.
- Misuse detectors provide systems administrators an easy to use tool to monitor their systems even if they are not security experts.

Disadvantages:

- Misuse detectors can only detect attacks known beforehand. For this reason the systems must be updated with newly discovered attack signatures.
- Misuse detectors are designed to detect attacks that have signatures introduced to the system only. When a well-known attack is changed slightly and a variant of that attack is obtained, the detector is unable to detect this variant of the same attack.

Misuse-based IDS used in our hybrid IDS is the open-source project Snort.

3.1.1. Snort

Martin Roesch, a software engineer working on the computer security topics, has developed Snort in 1990 in order to detect attacks targeting his home network. Snort is a fast, signature-based and open-source IDS. It produces alarms using misuse rules defined previously. It uses binary tcpdump-formatted files or plain text files to capture network packets. Tcpdump is a software program that captures network packets from computer networks and stores them in tcpdump-formatted files. Snort is rule-based and it has a language to define new rules. Snort is an open-source project and it has an architecture making it possible to integrate new functionalities at the time of compilation [6,22–24].