Computer Communications 49 (2014) 1–17

Contents lists available at ScienceDirect

Computer Communications

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

Review

False alarm minimization techniques in signature-based intrusion detection systems: A survey

Neminath Hubballi [a,*], Vinoth Suryanarayanan [b]

[a] Discipline of Computer Science and Engineering, Indian Institute of Technology Indore, India
[b] School of Computer Science, University of Birmingham, United Kingdom

ARTICLE INFO

Article history:
Received 23 September 2013
Received in revised form 25 April 2014
Accepted 27 April 2014
Available online 9 May 2014

Keywords:
False alarms
Correlation
Intrusion detection

ABSTRACT

A network based Intrusion Detection System (IDS) gathers and analyzes network packets and report possible low level security violations to a system administrator. In a large network setup, these low level and partial reports become unmanageable to the administrator resulting in some unattended events. Further it is known that state of the art IDS generate many false alarms. There are techniques proposed in IDS literature to minimize false alarms, many of which are widely used in practice in commercial Security Information and Event Management (SIEM) tools. In this paper, we review existing false alarm minimization techniques in signature-based Network Intrusion Detection System (NIDS). We give a taxonomy of false alarm minimization techniques in signature-based IDS and present the pros and cons of each class. We also study few of the prominent commercial SIEM tools which have implemented these techniques along with their performance. Finally, we conclude with some directions to the future research.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

In principle, computer systems need to be designed to prevent illegal access. However, mechanism to guard systems from illegal access is a non-trivial problem. An unauthorized mechanism designed to access system resources and/or data is called intrusion and designers are called intruders. Intruders can be classified as *Internal Intruders* and *External Intruders*. *Internal Intruders* attempt to elevate their limited privileges by abusing it. *External Intruders* attempt to gain unauthorized access to system resources from outside the target network. One of the earliest work on intrusion detection in computer networks is presented by Anderson [1]. In the seminal article, the author presents a threat model which describes internal penetrations, external penetrations and misfeasance. Further, the paper discusses a surveillance system for detecting all the three types of activities. In another major work, Denning [2] describes that users have a defined set of actions and intrusions can be detected assuming the intrusions deviate from the defined set of actions.

In recent days, computer security breach events due to intrusions are increasing. An Intrusion Detection System (IDS) monitors the system activity and reports on observation of any security violations. Traditionally there are two broad classes of IDS such as signature-based and anomaly-based. The former uses a database of known attack signatures and raises an alarm whenever network traffic matches any signature [3], whereas the later uses a model of normative system behavior and observable deviations are raised as alarms [4].

Whenever an attack is detected IDS generally raises an alarm to the system administrator. The alarm contains the information describing what attack is detected, who are the target and victims of the attack. The content associated with IDS alarms varies to a great extent depending on the nature of data (host or network) and also on the type of IDS mechanism (signature or anomaly). Signature-based IDS generates rich information along with alarm whereas anomaly IDS may just identify the connection stream which is detected as malicious.

The major concern with these systems is that, they attempt to detect suspected events which results in high false alarm rate (they account up to 99% [5–8]). Studies in [9,10] found the problem of false alarms by Snort even in the DARPA 99 dataset [11] which is generated in a controlled laboratory environment. The reason attributed for this alarming number of wrong detection is because many IDS detect too many suspicious cases. In a sense, suspected events are not necessarily intrusions to the system. An IDS with improper ruleset may miss some genuine intrusions. In the IDS literature, these cases are generally termed as false alarms. False positives and false negatives indicate whether detection is

* Corresponding author.
E-mail addresses: neminath@iiti.ac.in (N. Hubballi), vinothsuryanarayanan@gmail.com (V. Suryanarayanan).

http://dx.doi.org/10.1016/j.comcom.2014.04.012
0140-3664/© 2014 Elsevier B.V. All rights reserved.

spurious or a failure respectively. In the context of this paper we define the following terminology.

- *Attack:* Any malicious attempt to exploit a vulnerability, which may or may not be successful.
- *False positive:* False positive is generated when IDS raises an alarm for an unsuccessful attack attempt.
- *False alarms:* Set of false positives.

There are various reasons for false alarm generation in IDS and some of the important ones are listed below.

- Intrusion activity sometimes deviates very slightly from the normal and some cases are difficult to differentiate.
- Often the context in which a particular event has happened decides the usefulness of the alarm generated by that event. For example, "Microsoft Distributed Transaction (MDT)" service was vulnerable to intrusion of large packets, which was generating a buffer overflow. This triggers a denial of service for the MDT service. However, this vulnerability was exploitable only in the Windows 2000 operating system which was not patched with latest patches.
- Certain actions which are normal may be malicious under different prevailing circumstances. For example, network scan is normal if done by a security administrator otherwise it is abnormal.
- Many IDS not only detect intrusions but also the number of attempts of intrusions. An attempt may not necessarily lead to a compromised system. These alarms are very likely to overwhelm the administrator.
- An alarm may represent a stage in a multistage attack which may eventually fail due to various other reasons.

In addition to the above general reasons there are many reasons attributed for false alarm generation in a signature-based IDS.

- Often it is difficult to write good quality signatures [12]. A signature should be able to detect all possible variations of a pertinent attack and do not detect all non-intrusive activity. If a signature fails to match a pertinent attack it is considered as a false negative. On the other hand, if it matches for non-intrusive behavior a false positive is generated. This misinterpretation can happen under two situations.
  - Analyzing the irrelevant portion of traffic for finding a match.
  - Analyzing the wrong application data for finding a match.
- Signature writing is highly dependent on the expert knowledge. As discovery of new flaws and vulnerabilities occur continuously, to write good signatures one needs to have complete understanding of the behavior and also sufficient data to analyze. Due to this dependency, this method is always error prone.
- In most of the cases, IDS will run with default set of signatures which are not customized to the local network. Most of the vendor supplied signature databases come with a bundle of known attack signatures. The database entries should be minimized or customized based on the target system for operational efficiency. For example, if the target network has all systems running windows operating system, then signatures written to detect a Linux specific known attack can be removed.
- Latency in deployment of newly created signatures across all the IDS running computer systems is another reason. As soon as new signatures are written they need to be deployed in the signature database. Writing a signature requires expertise in understanding the semantics of attack. Thus vendor has to update signature database regularly.

Given the voluminous number of alarms, security managers often would like to prioritize alarms based on relevance and find out those alarms which have impact on target machine and defer decision on remaining alarm analysis to a later point of time or completely ignore them. This paper is a survey of such false alarm minimization techniques in signature-based intrusion detection system.

Rest of the paper is organized as follows. In Section 2, we review other related surveys and compare our work with them clearly justifying the motivation. Section 3 presents an overview of approaches for false alarm minimization in signature-based IDS. From Sections 4–11, we discuss various techniques used for false alarm minimization. In Section 12 we discuss hybrid approach of false alarm minimization which combines the best of some of the other techniques discussed in Sections 4–11 and in Section 13 we present a summary of various commercial SIEM tools in the market showing the methods currently in use along with their performance. Future research directions are presented in Section 14 with conclusions in Sections 15.

2. Prior work

An early survey [13] gives the generic architecture of alarm handling techniques. It discusses three aspects of alarm handling namely pre-processing, alarm analysis and correlation using IDMEF message format as a standard for data collection. In pre-processing step alarms are dumped into a relational database with a schema having attributes of IDMEF format. In the alarm analysis phase repeated alarms possibly coming from different IDS are removed and in final stage correlation of alarms is done. However, the study is very elementary and does not present the state of the art completely.

Limmer and Dressler [14] describe the event correlation technique from the perspective of early warning systems. The term event is used by the authors in a generic way rather than to mean IDS alarms. They refer events as the actual happenings in the network. For example, such events can come from net-flow data, port scan, IDS alarm and others like arrival of an ICMP packet, etc. They define event correlation as a technique of aggregating security related events in a centralized location and identifying relationship between them. This survey covers correlation architectures, attack intention identification, finding the scope of the attack and method of the attack. Correlation architecture can be either a centralized or distributed architecture. Attack intention is categorized either as scan, denial of service or exploitation. Scope of the attack as targeted or non targeted attack. Correlation algorithms are classified as *1*-pass, *n*-pass algorithms depending on how many times events are read by the correlation engine. However this paper does not discuss other techniques of false alarm minimization.

Sadoddin and Ghorbani [15] have given a survey of IDS alarm correlation techniques. This survey describes alarm correlation techniques from the alarm reduction point of view. Several stages of correlation are described. First one is normalization where alarms in different formats are brought into a common format, second being the aggregation in which multiple alarms are grouped and third one is correlation phase in which different correlation algorithms are used to find the relationship between the alarms. Prominent method for correlation being the Rule based correlation.

Download English Version:

https://daneshyari.com/en/article/447793

Download Persian Version:

https://daneshyari.com/article/447793

Daneshyari.com