Chapter 10

Intrusion Detection Systems Alerts Reduction: New Approach for Forensics Readiness

Aymen Akremi
Umm Al-Qura University, Saudi Arabia

Hassen Sallay
Umm Al-Qura University, Saudi Arabia

Mohsen Rouached
Sultan Qaboos University, Oman

ABSTRACT

Investigators search usually for any kind of events related directly to an investigation case to both limit the search space and propose new hypotheses about the suspect. Intrusion detection system (IDS) provide relevant information to the forensics experts since it detects the attacks and gathers automatically several pertinent features of the network in the attack moment. Thus, IDS should be very effective in term of detection accuracy of new unknown attacks signatures, and without generating huge number of false alerts in high speed networks. This tradeoff between keeping high detection accuracy without generating false alerts is today a big challenge. As an effort to deal with false alerts generation, the authors propose new intrusion alert classifier, named Alert Miner (AM), to classify efficiently in near real-time the intrusion alerts in HSN. AM uses an outlier detection technique based on an adaptive deduced association rules set to classify the alerts automatically and without human assistance.

INTRODUCTION

With the growth of digital world, malicious viruses or generally digital attacks are in continuous spreading using different methods and techniques making their detection very hard especially for unknown attacks which are malicious threat that their signature and updating security provisions databases or exploited vulnerability are not determined yet. Therefore, the compromised systems are seriously damaged.

DOI: 10.4018/978-1-5225-5583-4.ch010
Intrusion Detection Systems Alerts Reduction

Vulnerabilities may occur due to several factors such as human breaking of security policies which in turn may be exploited by malicious threats. The anomaly based intrusion detection systems are known by their high accuracy of unknown attacks detection since each new network behavior is considered as an attack. This feature makes anomaly-based intrusion detection systems largely used by organization and governments to protect from digital attacks and specially unknown attacks.

However, the use of data gathered from IDS for forensics purposes has initiated several discussions (Sommer, 1998; Stephenson, 2000; Yuil, 1999). The challenge is how much the IDS can meet and respect legal requirements in terms of integrity and original data preservation when collecting evidence during ongoing attacks. Although IDSs are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigation (Sommer, 1998), Yuil et al (Yuil, 1999) claimed that the IDSs are able to collect enough information during an ongoing attack to profile the attacker. The IDS may help detecting attacks in an early stage and therefore giving the opportunity to improve the readiness of the forensics system. Also, it links attack to events and gives a profound understanding of the attack type and targeted component which facilitates the suggestion of hypothesis about the suspect and help locate in advance the files and logs to be analyzed. The proposed digital forensics framework for SOA should include a smart log manager system allowing the collection, integration, reduction, and manipulation of the gathered logs from different components and security tools as IDS. However, IDS are known by their tremendous amount of the security alerts due to the high speed alert generation throughput and sensitivity to new network behavior which make the forensics management of intrusion detection alerts both compute and memory intensive. Obviously, the high level rate of wrong alerts reduces the performance and efficiency of IDS which minimizes its capability to prevent attacks and make the alert analysis tasks very difficult and time consuming.

In this chapter, we focus on the design and the implementation of an efficient IDS alert classifier that helps investigators to analyze the gathered data in real or near real time and improve the live forensics readiness to be used by the log management system under the log reduction and manipulation. More specifically, we propose Alert Miner; a classifier using a new alert classification algorithm based on a frequent pattern outlier detection data mining approach. The rest of this chapter is organized as follows: section 2 presents related work to IDS alert classification, section 3 shows the IDS alert processing model and the main data mining techniques used in the network specification extraction and classification improvement and section 4 presents the algorithm description. Section 5 shows the results of our implementation and our performance study. Finally, in section 6, we conclude the chapter by discussing the proposed approach, and proposing some future works.

RELATED WORK

Digital security attacks are being more sophisticated, unpredictable and frequent. Their danger is becoming more serious with the emergence of High-Speed Networks like Infiniband and Gigabit-Ethernet. New serious management problems mainly related to real time constraints, scalability, efficiency and portability raise key challenges to Intrusion Detection Systems successful deployment until now. More specifically the tremendous amount of security alerts due to the high speed alert generation throughput make the management of intrusion detection process both compute and memory intensive. Obviously the high level rate of wrong alerts degrades performance and efficiency of IDS which reduce its capability to prevent attacks and make the alert analysis tasks very difficult. Intensive research efforts have been