Journal of Information Security and Applications 41 (2018) 103–116

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A novel honeypot based security approach for real-time intrusion detection and prevention systems

Muhammet Baykara, Resul Das*

Department of Software Engineering, Technology Faculty, Fırat University, Elazığ 23119, Turkey

ARTICLE INFO

Article history:

Keywords:
Intrusion detection and prevention systems (IDS/IPS)
Honeypots
Network security
System security
Network traffic visualization

ABSTRACT

In the digitalized modern world in parallel to the new technological developments, information security has become the highest priority in the individual and institutional sense. In order to ensure the security of information systems, various systems are used techniques and technologies, including encryption, authorization, firewall, honeypot based systems. In this study, a honeypot based approach for intrusion detection/prevention systems (ID/PS) is proposed. The developed honeypot server application is combined with IDSs to analyze data in real-time and to operate effectively. Moreover, by associating the advantages of low and high-interaction honeypots, a superior hybrid honeypot system is performed. Therefore, in order to reduce the cost of configuration, maintenance, and management, after viewing the usage of honeypots on corporate networks, virtualization technologies are used. The developed system is a honeypot based intrusion detection and prevention system (IDPS) type and it is able to show the network traffic on servers visually in real-time animation. Thereby, it provides system information easily. Finally, the developed system can detect zero-day attack due to the configuration of intrusion detection, which makes it superior in performance compared to other IDSs. This system also helps in reducing the false positive level in IDSs.

1. Introduction

On account of higher cybercrime rate in the developing technology era, the information security term has come to light. Information security guarantees the availability of the information during its movement from sender to receiver in a confidence and inaccessible way for unauthorized users without degenerating and changing [1–3]. The main reasons motivate intrusion activities to threaten information systems are the demand for fame, reputation, financial benefits and national community benefits [4,5]. For the purpose of providing information security, a wide variety of hardware devices and software tools can be used [5]. For the personal or institutional need, information technologies managers should establish a suitable design, provide the needed security solution, and maintain its integrity. Moreover, ensuring the effective and dynamic operational process of information systems is done via providing and maintaining the effectiveness of these security measures [6]. In parallel to the technological developments, a large variety of attacks against information systems has also been increasing. The known attack types, which have been recorded are saved in attack databases. Intrusion detection systems keep these databases up-to-date and provide personal and institutional computer systems to monitor possible attacks consistently. IDSs are just analysis and monitoring systems, they do not contain any intrusion prevention option [7]. Intrusion prevention systems (IPSs) are the software and hardware equipment that have been developed to detect and prevent malicious attacks when the attacks happen. IPSs, thereby, are positioned on network connection segments, where they are located to prevent malicious traffic. These systems monitor the traffic that includes attack signatures already determined on the network; when they match, IPSs will be able to manage packet drop and termination of TCP connection. Additionally, IPSs may protect information system against Denial-of-Service (DoS) attack statistically or by measuring the traffic against the ascribed limitation [4]. Studies in technical literature dictate that a management information security system is to have confidentiality, availability, non-repudiation, identification, integrity and logging specifications [8–12].

In this study, for real-time intrusion detection and prevention systems, a honeypot-based approach is proposed. The developed honeypot server application is able to analyze real-time data, as it has been combined with IDSs to provide the ability of effective detection level. The advantages of low and high interaction honeypots thereby are combined, thus, a superior performance hybrid honeypot system has been developed. The developed system

* Corresponding author.
E-mail address: rdas@firat.edu.tr (R. Das).

https://doi.org/10.1016/j.jisa.2018.06.004
2214-2126/

has been designed to reduce the cost of security in enterprise networks. Moreover, this developed system reduces the false positive level, which is one of the most significant disadvantages of anomaly-based IDS. In addition, this system is adaptable against zero-day security vulnerabilities. Thus, creating the possibility for the detection of new attacks that do not exist in signature databases, and allowing IDSs to update these signature databases.

The developed system is honeypot based IDPS type that visualizes the network traffic on servers in real-time animation, similar to the global live attack maps. Global live attack maps can be used to see real global attacks, especially in real-time. Our developed system presents a live attack map of a real server traffic as an instance of a campus network, which can be used by any corporate or institutional network as well. According to the surveyed literature and up to the authors' knowledge, there is no any institutional honeypot-based intrusion detection and prevention system that shows both internal and external attacks together. From this point of view, this study provides an effective and a novel approach for the visualization of internal and external attacks on a corporate network.

2. Related work

The application of honeypots in security systems is neither meant for intrusion detection not is it incorporated in firewall to solve a particular security problem. In reality, the use of honeypots in security systems is mainly based on particular problem types and the solutions offered to these problems depend on aimed usage and targeted design [13,14]. Thus, compared to various information security systems, honeypots are not ought to provide a general response to all security issues [17,18]. In the technical literature, various security applications, such as IDPS, are used in a collective manner [17–22].

A VoIP-based low interaction honeypot was developed by Riboldi and his colleagues to detect malicious activities in their system. In their work, they deployed the monitoring of SIP protocol over 92 days to ultimately collect a total of 3502 events. Here, the authors developed their system in a way that simulates a firewall and IDS VoIP environment [24]. The concept of honeypots was used by Shukla et al. for the detection of unsafe web URLs. In their work, the developed system, using Python programming language, is set at the client side. They deployed a crawler on the client side that collects URL addresses, then it inspects if there is a legitimate need for a visit, it allows the websites to be visited. The inspection here is based on signature, thus, if a URL is considered risky or a source of vulnerability, a trigger is activated by IDS. Therefore, any suspicious URL address is saved in the blacklist, which enhances the security level of the system [25].

In another scenario investigated by Koniaris et al. the concept of honeypots was used for analyzing and visualizing malicious activities as well as connections. In this study, Koniaris and his colleagues deployed couple honeypots for alternate search purposes. One of the set-up honeypots was used for self-propagation option, aiming at detecting malicious software, while the other was made a trap to collect malicious activities [26]. Li et al. developed and set up an IDS which is based on a mixed interaction honeypot. In their work, they elaborated the role of the developed system in stabilizing the network and enhancing the overall security. As an outcome of their work, they could increasing the trapping ability of honeypot system, as measured by a number of research attempts [27]. Investigating new vulnerabilities using honeypots was approached by Chawda and Patel where they proposed a distributed honeypot system for this purpose. In this work, the employed honeypot is a low interaction type, and it is used as a front-end content filter [28].

Suo et al. elaborated the implementation of honeypot concept in IDSs. In their work, a proposal for eliminating IDS issues using honeypots was presented [29]. Apart from that, Paul et al. developed signature-based generator using a honeypot to secure computer network environment. One of the main aims of this work is to protect against attacks generated by the polymorphic worm. In addition, the proposed approach was useful for traffic classification, where the suspicious traffic was isolated and used for gather information on various attacks, especially work attacks. Further, in the developed signature-based system, when the system is unable to detect new attacks for unknown worm types, it would generate signature that suite this specific purpose [30].

Some of advantages of virtualization technologies were exploited by Beham and his colleagues where they investigated the idea of incorporating honeypots with both intrusion detection and nested virtualization systems. Essentially, the study conducted a comparative analysis between the current honeypot systems, nested virtualization technologies, and Virtual Machine Introspection (VMI) based intrusion detection [31]. Apart from that, an IDS based on a honeypot that deploys an IP tracing technique is proposed by Liu et al. In their study, they also proposed a design for intrusion detection system that presents the limitation of conventional IDSs on honeypot systems [32]. In the study of Pomsathit, the leveraging of honeypot systems and IDSs on distributed networks was addressed. The main aim of this study is to evaluate the how effective it becomes when combining both honeypot and IDS systems [33].

The application of a honeypot system suitable for enterprise business networks environment is provided in the study of Jiang et al. In their study, they deployed both IDSs methods as well as a new honeypot system to come up with an up-to-date honeypot system [34]. In another scenario, a scalable honeypot client which is performance-efficient and high interactive is designed by Akiyama et al. The purpose of their study is to establish an in-depth analysis and therefore increasing the capturing capability [35]. An autonomous version of honeypot implementation was tackled by Fanfara et al. Here, the developed version had the ability to create virtual honeypots and, thus, rapidly increase the security level of distributed heterogeneous computer systems [36]. Furthermore, a honeypot system which is applicable to Wireless Sensor Network (WSN) was presented by Markert et al. In their study, they also provided an effective analysis of their system and elaborated the detection capabilities for both known and unknown attacks [37].

A method for malicious traffic isolation based on a honeypot system was proposed and presented by Musca et al. They further analyzed the traffic to establish an automatic-based attack signatures generation for the SNORT intrusion detection/prevention system [38]. The idea of malicious traces collection using honeypots is also presented in the work of Sadasivam and Hota In their study, they implemented several honeypots in a virtualized environment to gather to achieve this purpose [39]. Apart from that, the idea of low-interaction honeypot systems was proposed by Djanali et al. In their study, they considered these low-interaction honeypot systems for emulating special vulnerabilities, particularly those exploiting XSS and SQL injection attacks. In essence, the developed honeypot in this study attempts revealing the hidden attacker's identity [40]. The concept of automated honeypots is also investigated in the study of Haltaş et al. In their study, they proposed a novel automated bot-infected machine detection system based on BotFinder through Honeypots (BFH). The identification of infected hosts in a real enterprise network is done using a learning approach [41]. The classification of IP-based network traffic for the identifying of unwanted traffic was conducted using low-interaction honeypot systems and network telescopes [42].