Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 03 Issue: 04 ISSN: 2582-3078 July 2021
Available online at: http:// www.jartms.org

INSIDER THREAT DETECTION USING HONEPOTS

V.V.Bhavani , K.Lakshmi Prasanna , N.Yaminidevi , S.Poorna Chandra rao

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.

Keywords : honeypots , anaconda , telegram , firewall

****Correspondence authors***
V. V . Bhavani , Assistant professor , department of CSE,
Usharama college of engineering and technology,
Telaprolu ,
Email : bhavani.vanukurus@gmail.com
***K . Lakshmi Prasanna** , Department of CSE,*
Usharama college of engineering and technology,
Email : lakshmiprasannakaturi6@gmail.com
***N . Yamini devi** , Department of CSE,*
Usharama college of engineering and technology,
Telaprolu,
Email : yaminirymb2000@gmail.com
***S . Poorna Chandra rao** , Department of CSE,*
Usharama college of engineering and technology,
Telaprolu ,
Email : poornachandrarao@gmail.com

.

INSIDER THREAT DETECTION USING HONEYPOTS

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

DESIGN

WORKING PRINCIPLE

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].

LOCATION OF HONEYPOTS

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.

CODING PLATFORM

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

Figure

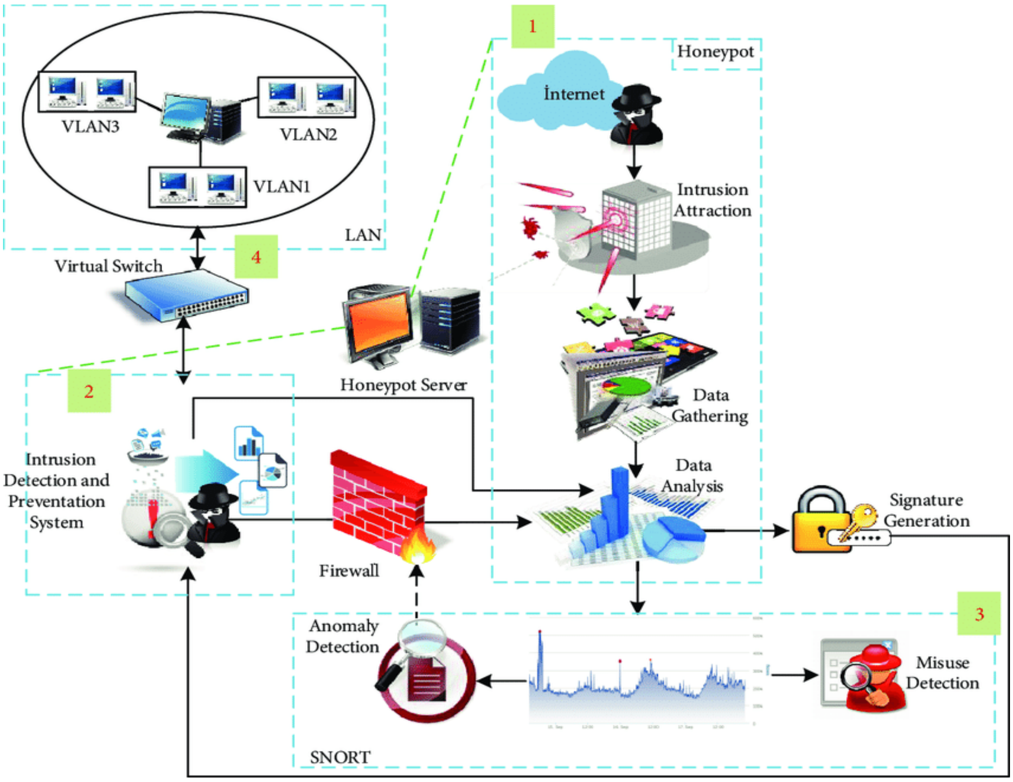

Fig-Server controls of honeypots

2. ANALYSIS

Honeypots are designed as software or as systems, which to locate networks and information security attacks, monitor the intruders' methods indicate the attack methods and initially to be aware of the new types of attacks [15]. The advantage of honeypots is drawn from their attackable status [16] in order to test their security vulnerability or simulate the security vulnerability response. In addition, they are positioned to attract the attention, as a hive for bees to make honey, as well as a trap pull the potential intruders. Honeypots do not generally have any significant or real information, therefore, attacking them is not considered as a threat. Compared to IDSs, IPSs and firewalls, honeypots do not provide a specific security solution on their own, rather they are considered as a part of security systems, and needed security solution determine the way they should be deployed [17]. The main purposes of honeypots deployment are specified as follows: • To acquire more insight about uncommon threats and vulnerabilities. • To act as a set-up trap system, where it attracts the attention of attackers. • To detect malicious activities on the network. • To form a protection for real systems by hiding them, and if any attack takes place, it would come to the honeypots. • To discover new attack types and methods (zero-day). Honeypots can be viewed in the content of information that they introduce to intruders. Some of such parameters can be information value and level, sources reachable by intruders and whether or not the honeypots are recognizable by intruders. Honeypots according to their interactivity level can be categorized into three groups: low, middle and high interaction [18]. Low and middle interaction honeypots operate in a way that attracts intruders via simulating the services that have security vulnerability [19,20]. They do not keep real and significant information. To implement such honeypots on a system, virtualization technologies can be used. Hence, the intruder has no direct access chance, hijacking the honeypots risk is so low. Since, the intruder does not get connected to the real system directly, less detailed information about the attack can be gathered. In low and middle interaction honeypots the simulation of the services is really significant. Here, errors occurred during the simulation process can help the intruder to detect the honeypot. The recognition of honeypots by attackers may create an undesired risk. Detecting the honeypot by intruders makes it lose its attraction and purpose. Unlike low and middle interaction honeypots, high interaction honeypots offer real services to attract the intruders will react .

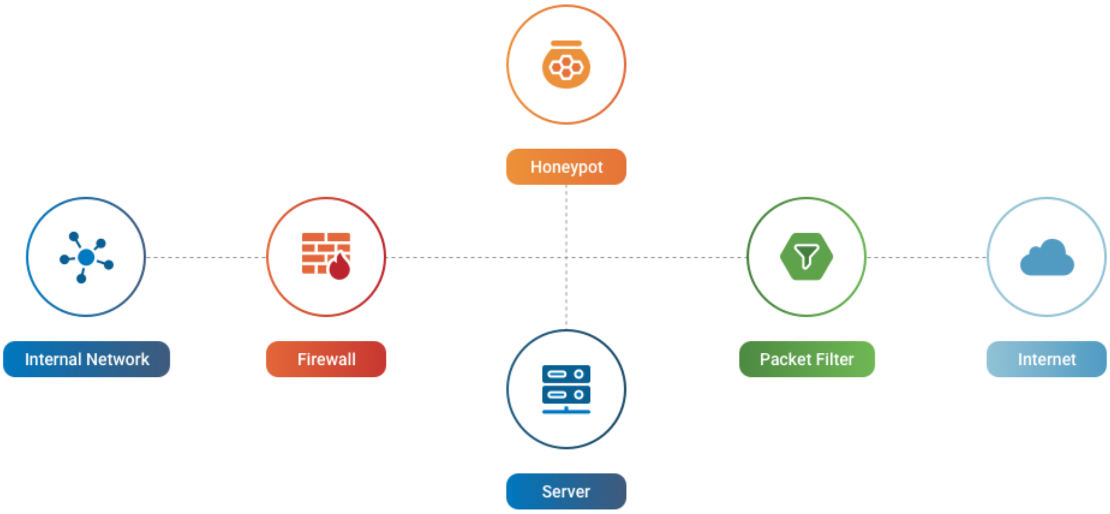

Fig-Location of honeypot

3. RESULTS

“Intrusion Detection Methods” where intrusion detection methods can be selected and “Help Wizard” menu. The performed IDS application has the ability to analyze packet and conduct protocol based analysis. By means of the application, it is possible to analyze the received packets by monitoring, intended port or network layer. These optional statuses are taken from the user via an interface. Fig. 4 shows “Honeypot Server Settings” window, where a new honeypot can be created. Fig. 5 presents the configuration process of the created honeypot. When a new honeypot is created and added to the server if there is another honeypot with the same named, the IDS application will not allow this operation to prevent possible errors, as shown in Fig. 4. PrP .

4 . CONCLUSION

In this study, a honeypot based approach is proposed, which can be used on the network security for the real-time intrusion detection and prevention systems. For this proposed novel approach, an effective software tool was developed. The developed system is a hybrid honeypot that combines the superior properties of low and high interaction honeypots in a single structure. The developed system has been tested on a simulated campus network in realtime, and successful results have been obtained. In this comprehensive study, by viewing the usage of honeypots on the enterprise networks, to reduce the installation, configuration, maintenance and management cost the virtualization technologies have been used. The network traffic that occurs on the honeypot servers can be visually monitored in an animation view. This provides information about the system in a convenient way. Based on our observation, in networks with VLANs, a machine with at least a different network interface for each VLAN should be deployed. The usage of a real machine for each VLAN, increases the costs of installation and maintenance especially for campus networks which deploy VLANs. For this reason, a central honeypot server application has been developed that enables honeypots to operate throughout the network with a network interface to reduce installation, configuration, maintenance and management cost. In the corporate with VLANs, a unique soft switch that is able to listen to layer-2 and layer-3 has been designed. Besides, the developed IDS application can be used as an IPS by connecting to the network as well as listening to the honeypot. For this purpose, signature-based intrusion detection methods can be integrated into the system. In the developed IDS application, using the open source sniffing tool SNORT IDS, a misuse detection.

REFERENCES

[1] B. I. Australia, “INFOGRAPHIC: everything that happens online in 60 seconds,” Business Insider. [Online]. Available: http://www.businessinsider.com/ infographic-what-happens-online-in-60-seconds-2015-5. [Accessed: 04-Apr2018].

[2] Pirounias S, Mermigas D, Patsakis C. The relation between information security events and firm market value, empirical evidence on recent disclosures: an extension of the GLZ study. Inf Secur Appl 2014;19:257–71. https://doi.org/10. 1016/j.jisa.2014.07.001.

[3] Pfleeger CP. The fundamentals of information security. IEEE Softw 1997;14:15– 16. 60 https://doi.org/10.1109/52.566419 .

[4] Safa NS, Maple C, Watson T, Von Solms R. Motivation and opportunity based model to reduce information security insider threats in organisations. J Inf Secur Appl 2018. https://doi.org/10.1016/j.jisa.2017.11.001.

[5] Bouabdellah M, Kaabouch N, El Bouanani F, Ben-Azza H. Network layer attacks and countermeasures in cognitive radio networks: a survey. J Inf Secur Appl 2018;38:40–9. https://doi.org/10.1016/j.jisa.2017.11.010

[6] Joshi C, Singh UK. Information security risks management framework – a step towards mitigating security risks in university network. J Inf Secur Appl 2017;35:128–37. https://doi.org/10.1016/j.jisa.2017.06.006.

[7] Li S, Rieck K, Woodward A. Special issue on threat detection, analysis and defense. J Inf Secur Appl 2014;19:163–4. https://doi.org/10.1016/j.jisa.2014.08.001.

[8] Fussell RS. Protecting information security availability via self-adapting intelligent agents. In: MILCOM 2005 - 2005 IEEE military communications conference, 5; 2005. p. 2977–82. https://doi.org/10.1109/MILCOM.2005.1606116.

[9] Shamala P, Ahmad R, Zolait A, Sedek M. Integrating information quality dimensions into information security risk management (ISRM). J Inf Secur Appl 2017;36:1–10. https://doi.org/10.1016/j.jisa.2017.07.004.

[10] Marcinkowski SJ, Stanton JM. Motivational aspects of information security policies. In: IEEE international conference on systems, man and cybernetics, 2003, 3; 2003. p. 2527–32. https://doi.org/10.1109/ICSMC.2003.1244263.