International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 5, September – October (2015)

SURVEY ARTICLE

A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems

Muhammet Baykara, Resul Daş
Firat University, Technology Faculty, Software Engineering Department, 23119, Elazığ/Turkey
mbaykara@firat.edu.tr, rdas@firat.edu.tr

Abstract – Information security in the sense of personal and institutional has become a top priority in digitalized modern world in parallel to the new technological developments. Many methods, tools and technologies are used to provide the information security of IT systems. These are considered, encryption, authentication, firewall, and intrusion detection and prevention systems. Moreover, honeypot systems are proposed as complementary structures. This paper presents the overall view of the publications in IDS, IPS and honeypot systems. Recently, honeypot systems are anymore used in connection with intrusion detection systems. So this paper describes possible implementation of honeypot technologies combined with IDS/IPS in a network. Studies in the literature have shown intrusion detection systems cannot find the 0-day vulnerabilities. The system provided by the honeypots and intrusion detection systems in the network, might detect new exploit and hacker attempt.

Index Terms – Information security, Intrusion detection system (IDS), Intrusion prevention system (IPS), Honeypot, Network Security.

1. INTRODUCTION

In parallel to rapid technological developments, a large variety of attack activities against to information systems have also been increasing. On account of higher informatics crimes rates in the technology, information security term has become more important. Attack types of which known and also have been recorded are saved in attack database. IDSs constantly, keep these database current and provide the personal or institutional computers systems to monitor possible attacks regularly and consistently. IDSs are just analysis and monitoring systems. They do not contain any intrusion prevention option. Studies in technical literature show that an information security management system is to have confidentiality, availability, nonrepudiation, identification, integrity and logging specifications [1-5].

In an information system or a network, any kind of unauthorized or unapproved and malicious activities are called intrusions [6]. An intrusion detection system (IDS) is a software application or a hardware that monitors network traffic and system activities for abnormal, malicious actions consistently [7]. IDS is a collection of the tools, methods, and resources to help identify, assess, and report intrusions [6, 8]. To provide information security encryption, authorization, firewall, intrusion detection and prevention systems are used. Also, as supplementary configurations honeypot systems are proposed.

Honeypots represent a real computer system, used as the trap for unauthorized communication in the network. Honeypot technologies are used combined with other security tools like IDS, IPS, firewall etc. The security systems that are composed of honeypots and IDS/IPS systems have higher performance especially for new vulnerabilities [9].

In this study, for real time intrusion detection and prevention systems, honeypot based approaches are investigated. Honeypot systems are combined with intrusion detection systems to provide the ability of work in an effective manner and actively in a network. In numerous study with the advantages of low and high interaction honeypots, a superior performance hybrid honeypot system are developed. Most of these system are designed to reduce the cost of security in enterprise networks. Moreover these developed system reduce the false positive level, which is anomaly based intrusion detection system that one of the most significant disadvantages and also they are able to adapt to against zero-day security vulnerabilities. Thus IDSs are able to detect a new attack that does not exist in signature database and are able to update signature databases when they are used with honeypot systems.

2. RELATED WORK

Honeypot systems are not used neither detecting intrusion detection system nor the firewall for a direct specific problem. Honeypots are used as a part of security systems and what kind of problem they will offer solution is depends on the design and usage purposes. Hence to the contrary other information security equipments it is not to be able to mention a honeypot that is able to give a general answer to every problem solution [10, 11]. In technical literature there are various security applications like intrusion detection and prevention (IDPS) are used collectively.

Riboldi et al. have developed a low interaction honeypot system to monitor illegal activities on VOIP systems in their study. During 92 days on the system whose performance has been monitoring, related to SIP protocol 3502 events have been gathered. They have interpretered their system as available like firewall and intrusion detection system VOIP environment [12]. Shukla et al. have performed a honeypot system to detect malicious web URLs in their studies. The system that has been developed by Python language is served in client side. By means of crawler on the client side the URL addresses are gathered and thereafter if there is a need for a visit, web sites are visited. If these URLs are malicious or contains vulnerability by the signature based intrusion detection system a trigger is activated. Thus the malicious URL addresses are saved in blacklist and so the security is available [13].

Koniaris et al. have used honeypot systems for the analysis and visualization of malicious activity and connections. In their performed application they have set up two alternate search honeypots. The first of these, generally has self-propagation option and has been intended to gather malicious software and the second has been intended to gather malicious activities as a trap system [14]. Song Li et al. have deliberated to set up a mixed interaction honeypot based intrusion detection system. They explain the purpose of the system that they have developed to stabilize the network and enhance the security. On account of enhancing network security they have increased honeypot system trap capability and have practiced a variety of researches [15]. Chawda et al. have proposed a distributed honeypot system to search new vulnerabilities. In their performed system to be exposed to further vulnerability as front end content filter they have used low interaction honeypot systems [16].

Xiangfeng Suo et al. have deliberated how to practice honeypot technologies in intrusion detection systems. In research work, they have submitted a proposal to practice honeypot systems to remove the intrusion detection system problems [17]. Paul et al. have performed a honeypot based signature generator for the computer network security. The developed system especially has been used for the purpose of protect against to polymorphic worm attacks. The developed system also has the skill to isolate suspicious traffic and gather many useful data about malicious traffic and worm attacks. When the signature based systems do not run to detect new attacks for the unknown worm attacks it has the skill to generate signature [18].

Beham et al. have benefited from the advantages of virtualization technologies. In their study, they have searched the intrusion detection and the nested virtualization environment of honeypot systems. In the study, current nested virtualization technologies, VMI based intrusion detection and honeypot systems have been searched comparatively [19]. Liu et al. have performed an intrusion detection system, which is honeypot based and uses IP traceback technique. To introduce the limits of conventional intrusion detection systems on honeypot systems an intrusion detection design has been offered [20]. Auttopan Pomsathit in his study, he has handled the usage of honeypot systems and intrusion detection systems on distributed networks. He has explained his main purpose has been measurement of effectiveness intrusion detection systems by using together both intrusion detection systems and honeypots [21].

Jiang et al. have handled honeypot system application for the enterprise business networks. They have combined the methods that are used in intrusion detection systems with a new honeypot system thereby to view current honeypot systems [22]. Mitsuaki et al. have designed a high interaction and effective performance scalable client honeypot. By this means in–depth analysis and capture capability have been aimed [23].

P.Fanfara et al. have focused on the technology called honeypot and the issue of implementation process of its autonomous version, which is able to create virtual honeypots and thus rapidly increase a security level of distributed heterogeneous computer systems in their study [24]. Markert J. et al. have presented an effective analysis of a honeypot for WSN and show detection capabilities in the categories of known and unknown attacks in their paper [25]. Musca C. et al. have presented methods for isolating the malicious traffic by using a honeypot system and analyzing it in order to generate attack signatures automatically for the SNORT intrusion detection/prevention system in their study [26]. Sadasivam G. K. et al. have deployed several honeypots in a virtualized environment to gather traces of malicious activities in their paper [27].

Djanali S. et al. have proposed a low-interaction honeypot for emulating vulnerabilities that can be exploited using XSS and SQL injection attacks. The proposed honeypot tries to overcome the techniques that hide the attacker identity [28]. Haltaş F. et al. have presented a novel automated bot-infected machine detection system BFH (BotFinder through Honeypots), based on BotFinder that identifies the infected hosts in a real enterprise network by learning approach in their paper [29]. Puska A. et al. have presented a method based on low-interaction honeypots and network telescopes for identification and classification of unwanted traffic on IP networks [30].

Bashir U. et al. have made a survey on the overall progress of intrusion detection systems in their paper. They survey the existing types, techniques and architectures of Intrusion Detection Systems in the literature. Finally they outline the present research challenges and issue [7].

Benmoussa H. et al. presented a survey of distributed Intrusion Detection Systems based on intelligent and mobile agents; it also proposes a new concept of proactive IDS in their study. At first, they introduce the topic. Then, they present limitations of classical IDSs. In the third part, they study the technologies of agent and multi-agent system and present benefits of using it to address shortcoming of classical IDSs. Finally, they present their approach and future work [8]. Dali L. et al. presented a survey on intrusion detection systems in their paper. First, they referred to different mechanisms of intrusion detection. Furthermore, they detailed the types of IDS. They have focused on the application IDS, specifically on the IDS Network, and the IDS in the cloud computing environment. Finally, the contribution of every single type of IDS was described [31].

Butun I. et al. presented a survey of the state-of-the-art in Intrusion Detection Systems (IDSs) that are proposed for WSNs in their study. Firstly detailed information about IDSs was provided. Secondly, a brief survey of IDSs proposed for Mobile Ad-Hoc Networks (MANETs) was presented and applicability of those systems to WSNs were discussed. Thirdly, IDSs proposed for WSNs were presented. This was followed by the analysis and comparison of each scheme along with their advantages and disadvantages. Finally, guidelines on IDSs that are potentially applicable to WSNs were provided. Their survey was concluded by highlighting open research issues in the field [32].

Torrano-Gimenez C. et al. presented a new system for web attack detection in their study. It follows the anomaly-based approach, therefore known and unknown attacks can be detected. The system based on a XML file to classify the coming requests as normal or abnormal. The XML file, which is built from only normal traffic, contains a description of the normal behavior of the target web application statistically characterized. Any request which deviates from the normal behavior is considered an attack. Their system has been applied to protect a real web application. They use an increasing number of training requests to train the system [33].

A many variety of researches and studies have been done for information security [35-40]. As it seen in current technical literature, to provide information systems and network security, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls and honeypots are not used just themselves alone. When the current studies, which are related to the subject is viewed security systems like those, hybrid designs that interaction with each other is seen proposed.

Within this study in our investigated applications also considering the proposals in technical literature, honeypots, intrusion detection and prevention systems are used together. Thus security system performance has been grown and especially false positive level, which is one of the most significant disadvantages of anomaly based intrusion detection system, has been reduced and unknown new attack patterns detection has been possible with these studies.

3. INTRUSION DETECTION SYSTEMS

An intrusion can be defined as any set of activities that attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signatures any of intrusions and malicious attacks. Intrusion Detection System (IDS) is a software or hardware system to provide the intrusion detection process automatically [8].

IDSs are classified according to many different criteria to the present day. Well-known classification criteria is intrusion detection method. IDSs are divided into two groups according to intrusion detection method as "anomaly detection" and "misuse detection".

3.1. Misuse Detection

Misuse detection method is also known as signature based detection. Figure 1 shows logical diagram of misuse detection.

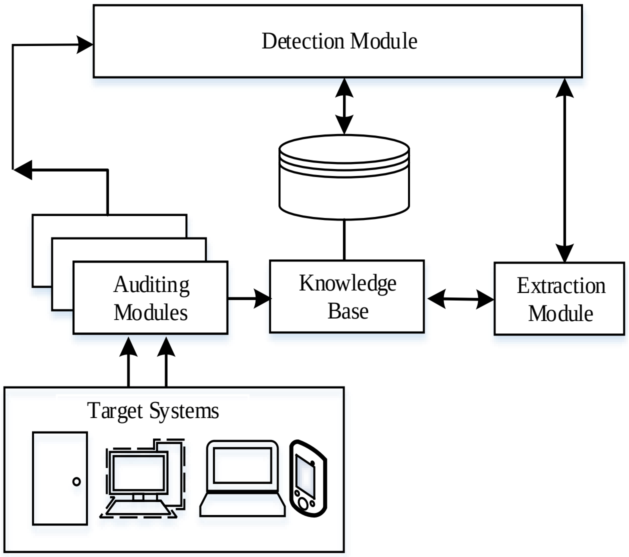

Figure 1 Misuse Detection [34]

Misuse detection method is based on a predefined set of attack patterns called "attack signatures" to look for attack traces. The predefined attack signatures are listed in a database as a detection rule. One of the principal benefits of using misuse detection is the detection of known attacks with a low false positive rate. On the other hand, misuse detection has two major disadvantages: the first one is that only known attacks can be detected. This provides a higher rate of false negative. The second one is that this technique must have a signature database defined for all of the possible attacks. This requires regular updates of signature database [8]. Figure 2 shows flowchart of misuse detection approach.

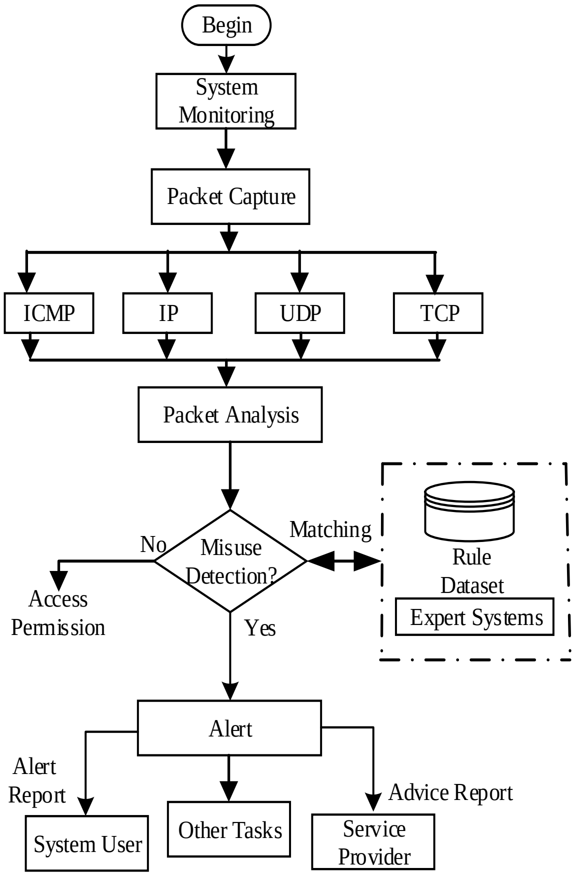

Figure 2 Misuse Detection Flowchart

3.2. Anomaly Detection

Anomaly detection approach consists of two phases: firstly a training phase which is based on the identification of normal traffic and behavior by constructing profiles of users, servers and network connections; and a testing phase where the learned profile is applied to new data [8]. Subsequently, any activity that deviates from this profile is considered as an intrusion. The main advantage of this approach is the capacity to detect new attacks without a priori knowledge of these attacks. These, unknown attacks can be detected. However, the system must go through a training phase to create the "normal" profile and it is not an easy to get this profile. Moreover, anomaly-based IDS flags many false alarms. The concept of false alarms can be classified into: false negative and false positive. A false positive is defined as an alarm being raised for legitimate activity and a false negative is defined as no alarms being raised for a real attack [7]. A many variety of techniques have been used for the anomaly detection problem, including statistical methods, expert systems, data mining, genetic algorithms, artificial neural networks and immune systems [8].

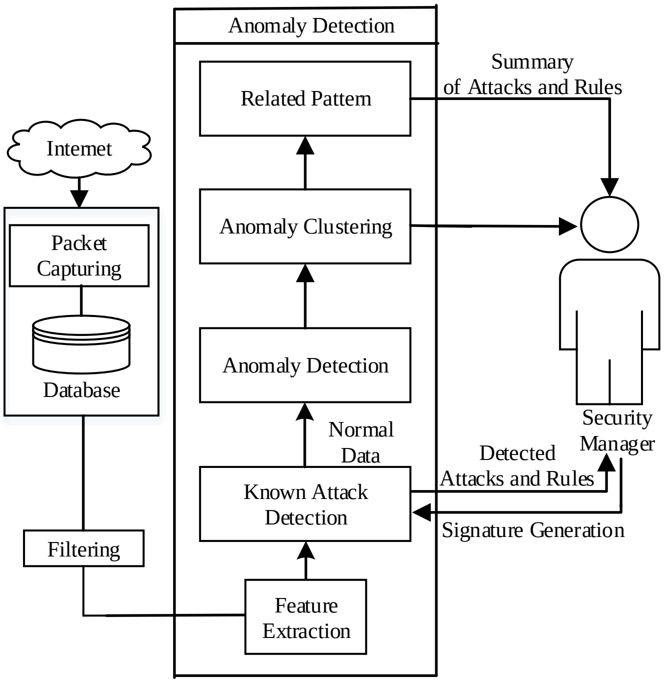

Figure 3 Anomaly Detection

Figure 3 shows logical diagram of anomaly detection. And also figure 4 shows flowchart of anomaly detection approach.

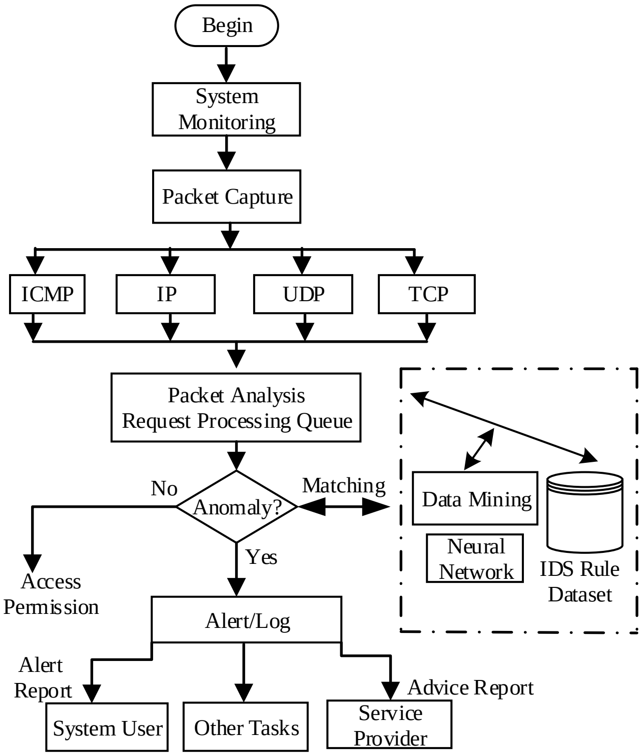

Figure 4 Anomaly Detection Flowchart

4. HONEYPOT SYSTEMS

Honeypot systems are designed to attract intruders. These systems are used as a trap for unauthorized communication in networks. Also honeypot systems are used to learn about intruder behavior and intrusion patterns. They are not used to solve a specific problem like firewall or IDSs. Honeypot systems are used as a part of security systems with other tools. With using honeypots, after an intrusion, network administrators or security officers can determine how the attacker succeeded, prevent subsequent attacks, and identify security vulnerabilities in the network. Besides identifying the various tools used by hackers, honeypot technology can also identify the social networks of intruders by determining the relationships among intruders [15].

4.1. Honeypot Types

There are some types of honeypot systems based on the amount of interaction. According to level of interactivity, honeypots are divided into three groups, as low, middle and high-interaction.

4.1.1. Low-Interaction Honeypots

These types of honeypot are limited in their degree of interaction. These systems actually simulate services and operating systems. In these systems, intruder's activities are limited to the level of emulation by the honeypot [16]. Low-Interaction honeypots represent a system which simulates specific protocols of TCP/IP model. They emulate open ports such as FTP, HTTP, SQL. Low-Interaction honeypots don't keep real or important data on them. They need minimal system requirements. It is the main advantage of low-interaction honeypots [9]. Figure shows low-interaction honeypot system. As it seen in Figure 5 the honeypot simulates the services and operating system.

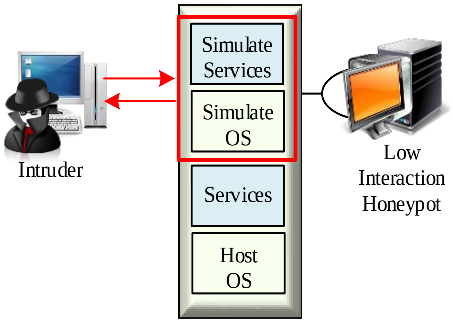

Figure 5 Low-Interaction Honeypots

4.1.2. Middle-Interaction Honeypots

Middle-interaction honeypot is a combination of low and high-interaction honeypot systems. This type honeypot is not only an emulation of the protocol. The attackers are not in communication with the real system in low and middle-interaction honeypots. So less detailed information can be taken from these types of honeypots. The protocols of applications are not detailed simulated. So attackers think that it is the real system [9].

4.1.3. High-Interaction Honeypots

In high-interaction honeypots, it is wanted to attract the intruders by getting the real services run. In addition to this, external programs are used to monitor the intruder activities. In high interaction honeypots respect to low and middle honeypots as the intruder in interaction directly in the real system to seize the honeypot risk is superior. To avoid this issue on the firewalls some precautions can be taken. Besides the intruder is in communication with the system directly can be gathered more detailed information. As the services run in real way it is harder to detect honeypot for the intruder. In this architecture, by using virtualization technologies on a physical machine on the network quite a few honeypots can be positioned.

High interaction honeypots are more costly and they need maintenance more frequently. Besides their advantages they can be reason security vulnerabilities. The networks on which the high-interaction honeypots are used should be isolated completely and all security precautions also should be taken otherwise as the intruder in interaction with real system can penetrate to honeypot and seise the system so that new security threats can be occurred. As it seen in Figure 6, high-interaction honeypots are real computer systems with specific real vulnerabilities [9].

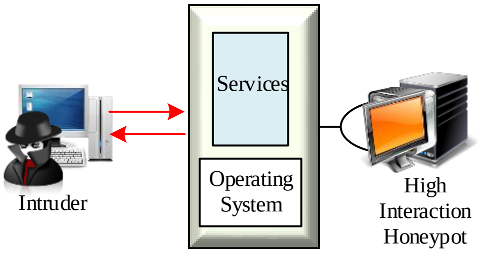

Figure 6 High-Interaction Honeypots

4.2. Honeypot Integration

There are three approaches for integration of honeypot technologies into the network. These methods contain positioning the honeypots in LAN, DMZ or Internet region of the network.

4.2.1. Honeypots in LAN Region

With positioning the honeypot systems in LAN region of a network, it is possible to include these systems into the network security. In this solution, honeypots are on the same segment as production servers. The main advantage of this scenario is that the honeypot can detect malicious attack both from Internet and local area network. If the network have VLANs, each

VLAN must have honeypot implementation [9]. Figure 7 shows the honeypot positioning in LAN region of the network.

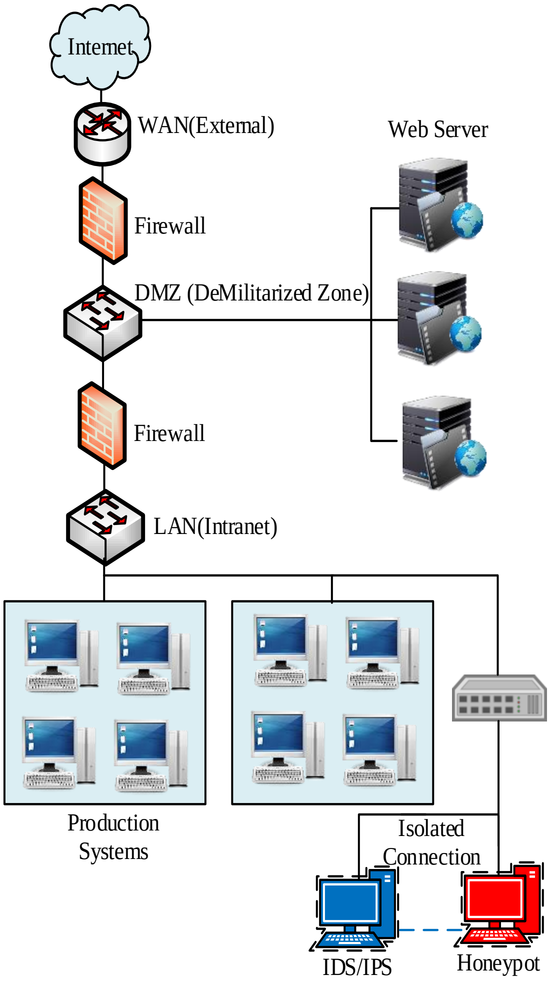

Figure 7 LAN Honeypot

As seen in Figure 7, the honeypot can detect malicious activities from outside and inside. It is known that in LAN region, located honeypot to seise causes significant security risks. So in this scenario, the attack attraction component of honeypot should be in low-interaction type.

4.2.2. Honeypots in DMZ Region

The main advantage of this type of location is isolation of the DMZ region from local area network. This scenario is not recommended as the only one solution for security. Because, the honeypot in the DMZ is not able to provide the security of hosts in the local area network. If there is any malicious attack to the local network, this type of honeypot could not detect them. In this situation, it is suggested to implement other honeypot in local area network [9, 15].

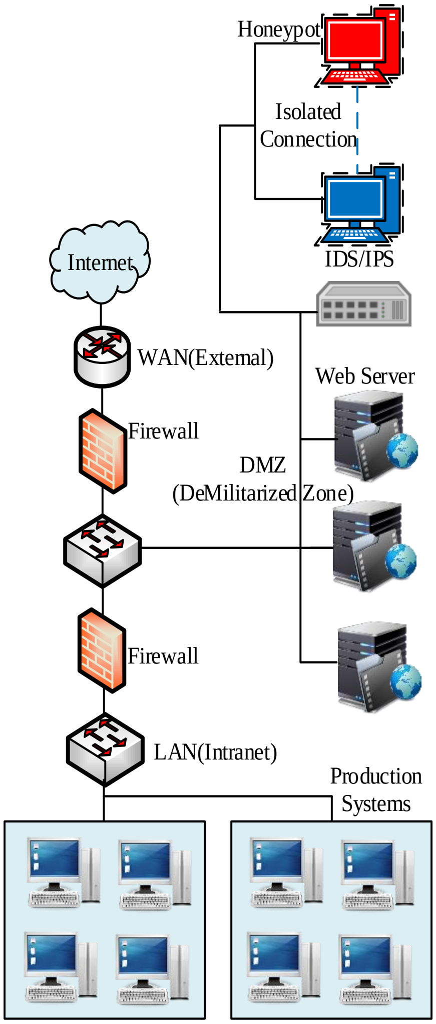

Figure 8 DMZ Honeypot

Figure 8 shows the schema of this solution. This location type is suitable to detect intruders in DMZ region. DMZ region contains production servers sometimes such as web server or mail server.

4.2.3. Honeypots in Internet Region

In this structure, activities on honeypot are monitored with IDS/IPS. To configure honeypot, to be isolated the network between IDS and honeypot, is important in this solution. Honeypot is not protected by any firewall. Because it is located directly on the internet region. In addition, honeypot is not allowed inclusion for security of LAN and DMZ region. In this approach, mostly external network attacks can be detected [9].

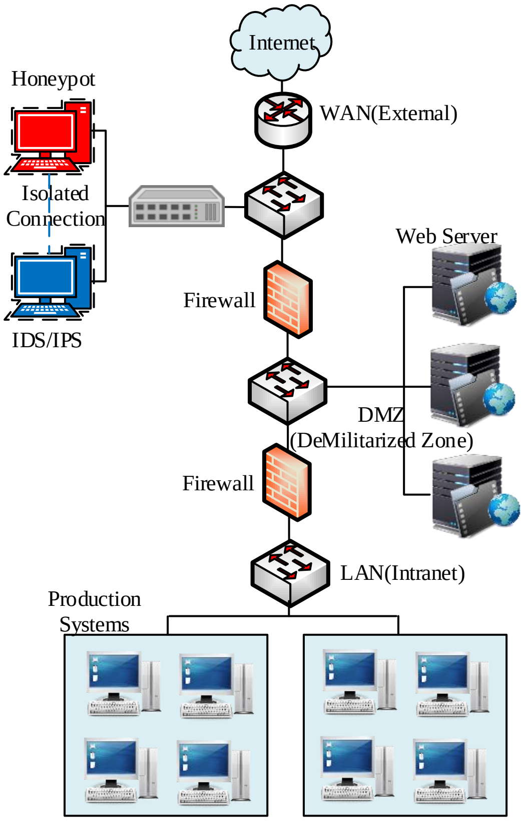

Figure 9 Internet Honeypot

This type of solution is positioning the honeypot in the internet region, outside of corporate network as seen in Figure 9.

5. HONEYPOT COMMUNICATION WITH IDS/IPS

Honeypot systems are complementary security tools, for IDS and IPS systems in a network. The studies in recent literature show that the intrusion detection systems are used in conjunction with honeypot systems. A general layout of the scenario which honeypot systems and IDSs are used together is given in Figure 10. As seen in Figure 10, honeypot systems can be used as a zero-day detection engine in this type of hybrid solution. Thus it can be detected previously unknown, new attacks. Because, almost all traffic on the honeypot is malicious.

Honeypots get their strength from their assailable option [10]. To form on their security vulnerability or simulate the security vulnerability response and also both to attract attention a hive bees to make honey and as a trap attract attention of the intruders, provide them to attack. Since they do not have real and significant information on them they do not become a threat in real terms. Unlike the other network and information security equipments like intrusion detection systems and firewalls, honeypots are not used for a specific problem solution. Honeypots are just a part of the security systems and their usage, at any problem solution is directly related to their designs and their usage way [11].

Honeypots combined with IDS/IPS systems main usage purposes specify below like;

- To have more knowledge of security vulnerabilities and intruder’s behavior.
- To detect the intruders and all unwanted traffic by means of set up trap system.
- To detect malicious activities that are on the network, and attacks from outside of the network.
- To hide the real systems, which are formed through the honeypots.
- To detect the new attack patterns and methods (zero-day).
- To make the system more secure.

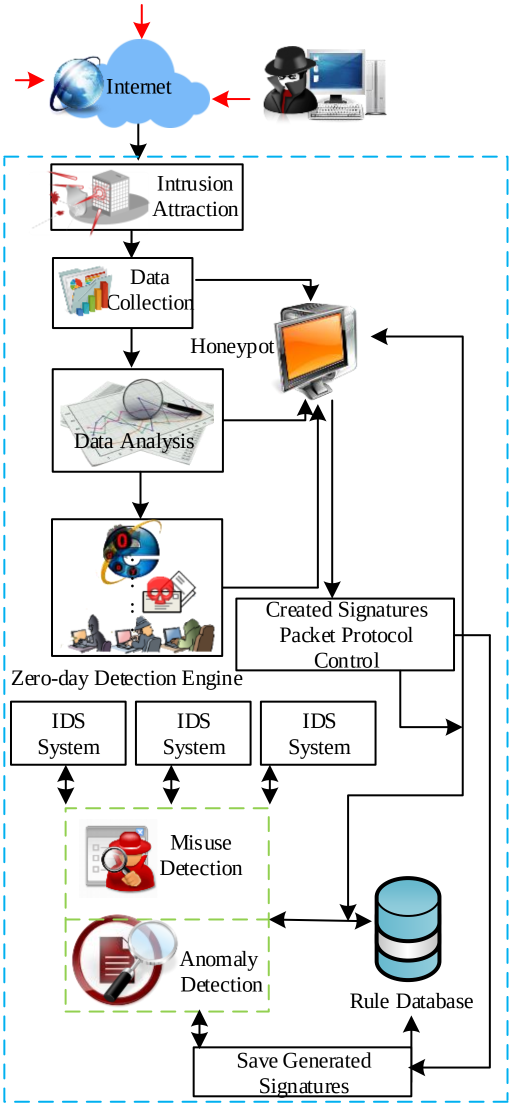

Figure 10 Honeypots with IDS/IPS

6. CONCLUSION

In this study, honeypot systems combined with IDS/IPS are investigated. The security tools such as IDS, IPS and firewall are not enough to be used alone. To provide a well-performed security system, honeypots are able to analyze real time malicious attacks combined with these tools. In numerous study with the advantages of low and high interaction honeypots, a superior performance hybrid honeypot system were developed. These systems provide minimal cost of security in corporate network. And these systems reduce the false positive alarm level, which is the most important disadvantages of anomaly based intrusion detection systems. And also they are able to adapt to against zero-day security vulnerabilities. Thus IDSs combined with honeypot, are able to detect new attack patterns that do not exist in signature database.

Within this study in our investigated applications also considering the proposals in technical literature, honeypots, intrusion detection and prevention systems are used together. Thus security system performance has been grown and especially false positive level has been reduced and unknown new attack patterns detection has been possible with these studies. If there are many VLANs inside the network, it is necessary to implement honeypots inside into each network. When the enterprise and honeypot designs viewed on the VLAN configuration used web systems, for each VLAN a device should be used, which has at least one different network interface. The usage of a real device for each VLAN, increases the costs of particularly including campus networks extended the enterprise network where the honeypots practiced entire web application, configuration, maintenance and management.

For this reason, to reduce installation, configuration, maintenance and management costs on large scaled enterprise network via an interface, the honeypots provided, can be active on entire network, a central server application should be developed. In the enterprise network including VLAN, via a novel soft switch design, which can sniff layer-2 and layer-3, it is also proposed the VLAN network scan be monitored.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the financial support from the Scientific Research Projects Administration Unit of Firat University (FUBAP) for this study performed under project with grant no. TEKF.15.04.

REFERENCES

[1] Fussell, R.S., "Protecting information security availability via self-adapting intelligent agents," Military Communications Conference, 2005. MILCOM 2005. IEEE, vol., no., pp.2977-2982 Vol. 5, 17-20 Oct. 2005.

[2] Tekerek M., “Bilgi Güvenliği Yönetimi”, KSÜ Fen ve Mühendislik Dergisi 11(1), s. 132, 2008.

[3] Marcinkowski, S.J.; Stanton, J.M., “Motivational aspects of information security policies”, IEEE International Conference on Systems, Man and Cybernetics, vol.3, pp.2527-2532 vol.3, 5-8 Oct. 2003.

[4] Campbell, S., "Supporting digital signatures in mobile environments," Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. , vol., no., pp.238-242, 9-11 June 2003.

[5] Karaarslan, E., Teke A., Şengonca H., "Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması." Akademik Bilişim Konferansı, Çukurova Üniversitesi, 1s, 2003.

[6] Can, O.; Sahingoz, O.K., "A survey of intrusion detection systems in wireless sensor networks", 6th International Conference on in Modeling, Simulation, and Applied Optimization (ICMSAO), pp.1-6, 27-29 May 2015.

[7] Bashir, U.; Chachoo, M., "Intrusion detection and prevention system: Challenges & opportunities", International Conference on Computing for Sustainable Global Development (INDIA Com), pp.806-809, 5-7 March 2014.

[8] Benmoussa, H.; El Kalam, A.A.; Ouahman, A.A., "Towards a new intelligent generation of intrusion detection system", Proceedings of the 4th Edition of National Security Days (JNS4), pp.1-5, 12-13 May 2014.

[9] Malanik D., Kouril L., “Honeypot as the Intruder Detection System”, In Proceedings of the 17th WSEAS International Conference on Computer, Kos(GR), pp. 96-101, 2013.

[10] Gökırmak Y., Bektaş O., Soysal M., Yiğit S., “Sanal IPv6 Balküpü Ağı Altyapısı: Kovan”, Ulusal IPv6 Konferansı, 2011.

[11] Gökırmak Y., Yüce E., Bektaş O., Soysal M., Orcan S., “IPv6 Balküpü Tasarımı”, Tübitak Ulakbim, Ankara, 2011.

[12] Riboldi Jordao da Silva Vargas, I.; Kleinschmidt, J.H., "Capture and Analysis of Malicious Traffic in VoIP Environments Using a Low Interaction Honeypot," Latin America Transactions, IEEE (Revista IEEE America Latina), vol.13, no.3, pp.777-783, March 2015.

[13] Shukla, R.; Singh, M., "PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems," 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), vol., no., pp.1-5, 8-10 Oct. 2014.

[14] Koniaris, I.; Papadimitriou, G.; Nicopolitidis, P.; Obaidat, M., "Honeypots deployment for the analysis and visualization of malware activity and malicious connections", IEEE International Conference on Communications (ICC), vol., no., pp.1819-1824, 10-14 June 2014.

[15] Song Li; Qian Zou; Wei Huang, "A new type of intrusion prevention system, "International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), vol.1, no., pp.361-364, 26-28 April 2014.

[16] Chawda, K.; Patel, A.D., "Dynamic & hybrid honeypot model for scalable network monitoring," International Conference on Information Communication and Embedded Systems (ICICES), vol., no., pp.1-5, 27-28 Feb. 2014.

[17] Xiangfeng Suo; Xue Han; Yunhui Gao, "Research on the application of honeypot technology in intrusion detection system," IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA), vol., no., pp.1030-1032, 29-30 Sept. 2014.

[18] Paul, S.; Mishra, B.K., "Honeypot based signature generation for defense against polymorphic worm attacks in networks," IEEE 3rd International Advance Computing Conference (IACC), vol., no., pp.159-163, 22-23 Feb. 2013.

[19] Beham, M.; Vlad, M.; Reiser, H.P., "Intrusion detection and honeypots in nested virtualization environments,"), 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN, vol., no., pp.1-6, 24-27 June 2013.

[20] Liu Dongxia; Zhang Yongbo, "An Intrusion Detection System Based on Honeypot Technology," International Conference on Computer Science and Electronics Engineering (ICCSEE), vol.1, no., pp.451-454, 23-25 March 2012.

[21] Pomsathit, A., "Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Honeypot," Congress on Engineering and Technology (S-CET), vol., no., pp.1-4, 27-30 May 2012.

[22] Jiang Zhen; Zhenxiang Liu, "New honeypot system and its application in security of employment network," IEEE Symposium on Robotics and Applications (ISRA), vol., no., pp.627-629, 3-5 June 2012.

[23] Akiyama, M.; Kawakoya, Y.; Hariu, T., "Scalable and Performance-Efficient Client Honeypot on High Interaction System," IEEE/IPSJ 12th International Symposium on Applications and the Internet (SAINT), vol., no., pp.40-50, 16-20 July 2012.

[24] Fanfara, P.; Dufala, M.; Chovancova, E., "Usage of proposed autonomous hybrid honeypot for distributed heterogeneous computer systems in education process," IEEE 11th International Conference on Emerging eLearning Technologies and Applications (ICETA), vol., no., pp.83-88, 24-25 Oct. 2013.

[25] Markert, J.; Massoth, M., "Honeypot Effectiveness in Different Categories of Attacks on Wireless Sensor Networks,"25th International Workshop on Database and Expert Systems Applications (DEXA), vol., no., pp.331-335, 1-5 Sept. 2014.

[26] Musca, C.; Mirica, E.; Deaconescu, R., "Detecting and Analyzing Zero-Day Attacks Using Honeypots," 19th International Conference on Control Systems and Computer Science (CSCS), vol., no., pp.543-548, 29-31 May 2013.

[27] Sadasivam, G.K.; Hota, C., "Scalable Honeypot Architecture for Identifying Malicious Network Activities," International Conference on Emerging Information Technology and Engineering Solutions (EITES), vol., no., pp.27-31, 20-21 Feb., 2015.

[28] Djanali, S.; Arunanto, F.X.; Pratomo, B.A.; Baihaqi, A.; Studiawan, H.; Shiddiqi, A.M., "Aggressive web application honeypot for exposing attacker's identity,"1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), vol., no., pp.212-216, 8-8 Nov., 2014.

[29] Haltas, F.; Uzun, E.; Siseci, N.; Posul, A.; Emre, B., "An automated bot detection system through honeypots for large-scale," 6th International Conference on Cyber Conflict (CyCon 2014), vol., no., pp.255-270, 3-6 June 2014.

[30] Puska, A.; Nogueira, M.; Santos, A., "Unwanted traffic characterization on IP networks by low interactive honeypot," 10th International Conference on Network and Service Management (CNSM), vol., no., pp.284-287, 17-21 Nov. 2014.

[31] Dali, Loubna; Bentajer, Ahmed; Abdelmajid, Elmoutaoukkil; Abouelmehdi, Karim; Elsayed, Hoda; Fatiha, Eladnani; Abderahim, Benihssane, "A survey of intrusion detection system," 2nd World Symposium on Web Applications and Networking (WSWAN), pp.1-6, 21-23 March 2015.

[32] Butun, I.; Morgera, S.D.; Sankar, R., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, no.1, pp.266-282, First Quarter 2014.

[33] Torrano-Giménez, C., Perez-Villegas, A., and Álvarez Marañón, G., "An anomaly-based approach for intrusion detection in web traffic" Internet: http://digital.csic.es/bitstream/10261/40544/1/ARTICULOS315428%5B1%5D.pdf (2010).

[34] Gennaro Della V., Massimo E., "A Knowledge-Based Approach for Detecting Misuses in RFID Systems", Designing and Deploying RFID Applications, Dr. Cristina Turcu (Ed.), ISBN: 978-953-307-265-4, InTech, DOI: 10.5772/17535. Available from: http://www.intechopen.com/books/designing-and-deploying-rfid-applications/a-knowledge-based-approach-for-detecting-misuses-in-rfid-systems.

[35] Demirol, D., Daş, R., Baykara, M., "SQL Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu)", 62-66, 20-21 Mayıs 2013, Elazığ - Turkey.

[36] Karadoğan, İ., Daş, R., Baykara, M., "Scapy ile Ağ Paket Manipülasyonu", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu)", 196-201, 20-21 Mayıs 2013, Firat University, Elazığ - Turkey.

[37] Baykara, M., Daş, R., Karadogan, İ., "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu)", 231-239, 20-21 Mayıs 2013, Firat University, Elazığ - Turkey.

[38] Gündüz, M.Z., Daş, R., "Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (6th International Conference on Information Security and Cryptology - ISCTURKEY 2013), pp.302-307, 20-21 Eylül 2013, ODTÜ, Ankara.

[39] Gündüz, M.Z., Daş, R., "Kablosuz Yerel Alan Ağlarına Sızma Uygulaması ve Temel Güvenlik Önerileri", 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (7th International Conference on Information Security and Cryptology - ISCTURKEY 2014), pp.295-300, 17-18 Ekim 2014, İstanbul Teknik Üniversitesi, İstanbul.

[40] Bürhan, Y., Daş, R., Baykara, M., "Sosyal Ağ Ortamlarında Karşılaşılan Tehditlerin Analizi", The Third International Symposium on Digital Forensics and Security (ISDFS 2015), pp.194-200, 11-12 May, 2015, Gazi University, ANKARA.

Authors

Muhammet Baykara was born in Elazig, Turkey. He received his BS and MSc. in Computer Engineering from Firat University in 2006, 2009 respectively. Currently, he is a research assistant in the Department of Software Engineering at Firat University. He is pursuing his PhD degree in Software Engineering. His research interests are Information Security, Honeypots, Intrusion Detection and Prevention Systems.

Resul Das received his BS and MSc. in Computer Science from Firat University in 1999, 2002 respectively. He received PhD degree from Electrical and Electronics Engineering Department in same university in 2008. He is an Assoc. Professor at the Department of Software Engineering of Firat University, Turkey. He has authored several paper in international conference proceedings and refereed journals, and has been actively serving as a reviewer for international journals and conferences. His current research interests include Knowledge Discovery, Web Mining, Complex Networks, Computer Networks, Information and Network Security.