Honey Pot: A Major Technique for Intrusion Detection

Rajalakshmi Selvaraj, Venu Madhav Kuthadi and Tshilidzi Marwala

Abstract Generally, Intrusion detection system (IDS) is installed in industrial environment for protecting network that works based on signature, where they are not capable of detecting most unidentified attacks. The detection of undefined attack and intrusion is not more helpful to identify the several kinds of attack, where intrusion-based attack has become a challenging task to detect intruder on network. A skilled attacker can obtain a sensible information and data from the system after knowing the weakness. Distributed denial of service (DDoS) is a major thread over the security and most enlarging thread in recent days. There are so many types of Denial of Service (DoS) such as Teardrop, Smurf, Ping of Death, and Clone attack. The aim of the cyber defense system is to detect the main cause of the several counter attacks on the enterprise network. On the way to fix these issues, we are proposing a novel idea that relies on honey pot technique and packet data analysis which are trained by the sample of malware after using the Intrusion detection technique in both ways separately as Network and Anomaly intrusion detection system. Some approaches are not being easily implemented in the network of real enterprises, because of practicability training system which is trained by the sample of malware or deep analysis of packet inspection or depends on the host-based technique that requires a big capacity for storage over the enterprise. The honey pots are one of the most successful techniques to collect the sample of malware for

R. Selvaraj (✉) · T. Marwala
Faculty of Engineering and the Built Environment, University of Johannesburg, Johannesburg, South Africa
e-mail: selvarajr@biust.ac.bw

T. Marwala
e-mail: tmarwala@uj.ac.za

R. Selvaraj
Department of Computer Science, BIUST, Gaborone, Botswana

V.M. Kuthadi
Department of AIS, University of Johannesburg, Johannesburg, South Africa
e-mail: vkuthadi@uj.ac.za

S.C. Satapathy et al. (eds.), *Proceedings of the Second International Conference on Computer and Communication Technologies*, Advances in Intelligent Systems and Computing 380, DOI 10.1007/978-81-322-2523-2_7

the purpose of analysis and identification of attacks. Honey pot is a novel technology which consists of massive energy and possibilities in the field of security. It helps reading the behavior of the attack and attacker information.

Keywords Honey pot · IDS · Packet analysis · Intruder

1 Introduction

The computer system security is one of the most important areas of consideration in Information Technology (IT). There is a quick progress in this field because everyone wants to keep the information secure, and no one wants to leak their information to the Attacker by the intrusion and compromised data [1]. Recently, the internet has become a popular way to communicate with computers all over the world. When the constant Communication has been creating some new possibility, it also brings the several chances for the malicious-affected users. The significance of the security over network is growing, the IDS is one of the methods to identify the malicious behavior over the network [1, 2]. The numbers of internet users are increasing continuously per day. The internet traffic is getting high every day by the user crowd, so the internet security is mostly required in the recent days in the area of computing system. Honey pot system is developed for detecting and analyzing the malicious attack which tries to access the network. Honey pot is a machine that looks like a real database, server, and Operating System (OS) for the attackers. A Honey pot system attracts the attacker and it gives an invitation for attack. The goal of the honey pot is to secure the existence system from the attackers and gain the information of the attackers by creating a log case for their harmful activity by the specific IP address [3]. The attackers perform their work professionally in the automated and well-organized environment after controlling over the zombie machine for which network of the enterprise is preferable. As the infected systems are most dangerous in the cyber-attack, decontaminant of them is one of the main aims for Active Cyber Defense (ACD); thus, the initially step is inevitably analyzed. The effect of the Scalable and practical system is with the ability of standing growth and efficient identification of the malwares for detecting the infected machines [4]. The main aim of the honey pot is to identify the attacker and let them to access the network and store the information of the intrusion like IP address, TCP address, etc., and then divert their path to the fake database instead of accessing the real database. Nowadays, the intrusion detection is the big issue for the research behavior [5]. Honey pots are one of the strong agents to identify the attacker and capture the intruder information based on intelligence and black-hat behaviors. Some distinct services like IDS and firewall are signature-based services, and a lot of work has been done in the field of the signature-based detection. Therefore, the

honey pots are the one of the most interesting techniques for controlling the attack on the internet. It easily collects the information about the attacker. When compared to other technique, honey pot is reducing the risk of attack [6]. Once attacker reaches to the firewall system, then they will easily collect all the valuable data from the system and nothing will be remaining to save from them [7]. With the additional approach of Booby traps it is possible to prevent the weakness of the system and attracts the intruders to the system. This system starts interaction with the attacker and collects all the information of attackers. This latest technique is known as Honey pot [8]. The proposed method discussed about the intrusion aspects, origin, and cause and also included the information in detail for the packet sources. We are providing the several detection methods, tools, and systems for intrusion classification. We are not only focusing on the analysis and classification of IP traffic but also trying to focus on the several updated methods, tools, analysis, and systems.

2 Related Work

Jeremy et al. [9] have proposed a design of the high interaction over the honey pot to present a result with discussion. They have presented two types of honey pot host, the First class stops accessing the unauthorized users and reinstallation, and second class allows the reinstallation. The author of the [10], aimed to secure the information of the system from the attacker or unauthorized access against the DoS. This is gained by controlling the traffic of attack and mechanism of pushback. Vinu Das [10] proposed the honey pot on the basis of the distribution detection of attack from different sources of attack by using the traditional system of honey pot [11] and distributed consumption for enhancing the overall protection of system area. The system identifies the attacking behavior by the database feature invasion, which could be compatible with the snorting feature of library, and detecting the recent invasion features by real-time up-gradation. Divya et al. [12] developed IDS which contains hybrid honey pot with GA (genetic algorithm), where the high interaction of the attacker has been established with the unknown attackers. Yun Yang et al. [13] proposed an IDS with C4.5 DT (Decision Tree) algorithm. In this technique, intrusion creation rule gains the information over the attacker in ratio. The authors' experimental result produces that the IDS C4.5 algorithm is effective and feasible and the rate of accuracy is high. Jiqiang et al. [14] have proposed a note on the black-hat community services that make a harmful access in the system for stealing the secret information, where the honey pot system attracts the attacker and gain their information and store them. The honey pot is the most valuable for creating a new signature for detecting the intruders.

Rameshbabu et al. have proposed the Egress filtering technique to filter the [15] outbound traffic of network. Here, the author proposed an example related to the DoS attacks which can provide the details of intruders and prevent to access the attacks as well as provide the description of the filtering execution. Siva et al. [16] have proposed the techniques of utilizing the port hopping that communicates with

the parties of application over port. But here no pre-calculation procedure has been done which makes it easier to trace randomly.

3 Proposed Work

3.1 Overview

Honey pots are largely used in the security field for defecting, preventing, and detecting the breaches that abandoned the security measure, and make more efficient and accurate measurement for security purpose. The methods of honey pot consumption directly implement the role of honey pot in security system. Basically, honey pot is a mechanism of collecting and learning the information. Its main aim is not only to catch the black-hat community attacker and put charges over them but also the aim of it is to attract the attackers and hacker and collect information about them. This information will be helpful for the future study and attacking ideas. We are proposing a novel idea in our project called virtual honey pot, which will identify and catch the intrusion on the network shown in Fig. 1.

3.2 Intrusion Detection

3.2.1 Network-Based Intrusion Detection System

Network-based Intrusion Detection System (NIDS) observes the crowd flows over another host. Observing area in the network-based region can either enlarge or minimize the particular area with the related effort. Network-based intrusion detection system has a capability to stand against the crowd over network to maintain the effect. With the increasing traffic, the network-based IDS has to clear the traffic and observe in the manner of time.

3.2.2 Anomaly-Based Intrusion Detection System

Anomaly-based Intrusion Detection System (AIDS) observes the activity, transaction, outgoing traffic, and behavior to detect the intrusion by anomaly detection. It checks the behavior of users on the notion that is different from the normal behavior identified as an attacker. The administrator of the system sets the limitation of the normal behavior. AIDS is prone for the false positive. AIDS is causing the heavy process on the network system. We have two factors: first one is False Positive: Anomalies are signed as an intrusive when that is not an intrusive, and other one is False Negative: Anomalies are not signed as an intrusive when that is an intrusive.

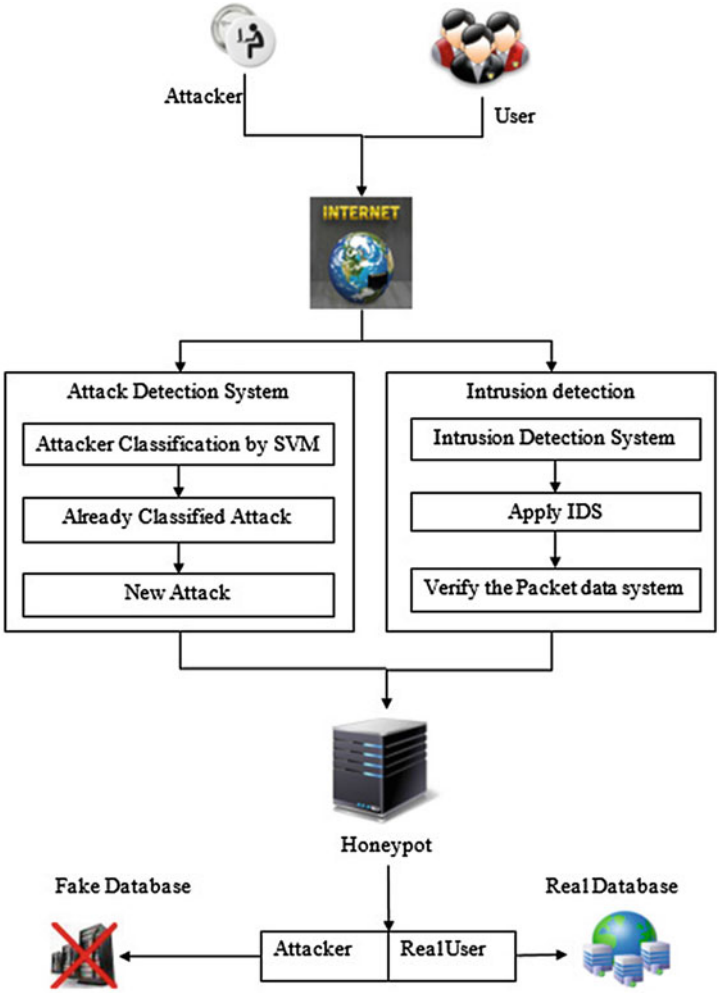

Fig. 1 Proposed honey pot architecture

3.2.3 Honey Pot

The honey pots are intended to imitate the systems to detect intrusion which has a tendency to break the intruder limit in accessing the overall network. When it is successful, then the attacker will not know that they are monitored and tricked. Most of the honey pot systems are installed inside the firewall so they can do better control over full network; however, it is possible to implement outside the firewalls. The firewall system within honey pot works in an opposite way: the honey pots are allowing the incoming attackers instead of blocking them and divert their path from

the real database to false database and restrict the function which attackers try to access.

3.2.4 Packets Analysis

These functions present an analysis for capturing the packet and exploring the information. This information consists of TCP, IP, ICMP, and UDP header. Then, the packet divides between two (source and destination) IP address and stores the records in each 4 s. It is functionally applied in every connection and defines the attack and normal behavior.

3.2.5 Support Machine Vector (SVM)

Support Vector Machines (SVM) is a classifier which was designed to classify the binary format. The application for classification will solve the problem based on the multi-class. SVM supports the decision tree which combines the decision tree and SVM that enhance a way to solve out the problem of multi-class. This technique is most effective and can decrease the timing of testing and training processes and increase the system efficiency. Some distinct way to create the binary trees will divide the set of data into the various subsets from the root to leaf till all subset merged into the one class. The creation of the binary tree function is having a huge power for the classification. For the construction of multi-class IDS, this research work implements a novel approach based on the DT.

3.3 Algorithm

3.3.1 Intrusion Detection System

IDS takes the packet as input from the network and also monitors the time slot of incoming flow. While monitoring the time slot and packet, IDS detects the malicious time slot and checks for the suspicious flow and extracts the malicious flow from the traffic, and it processes and generates the new filtering rule. Signatures are built from the filtering rule for intrusion detection.

IDS (P,T) = {FR, SGN,L2}
Where,
T = time slot,
FR = Filtering Rule.
SGN = Signature Created.
L2 = Log Report.

3.3.2 Honey Pot

The captured packets are used as an input in the honey pot and precede the packet to attain the information for every particular system from the origin of packet. Honey pot precedes the packet analysis and generated reply to engage the client system from host.

HP(P) = CLD + L1.
Where, client
P = {ICMP,TCP,UDP} = Set of packet entering to the system.
CLD = {cIP,PType,Preply} = client details.
cIP = client IP.
PType = packet type.
Preply = Reply packet.
L1 = Log Report

3.3.3 Packet Analysis

Algorithm

1: Begin to receive packets
For every packet p
if (Received_protocol == Transmission Control Protocol)
Infer features of Transmission Control Protocol extract
else
if (Received_protocol == User Datagram Protocol)
Infer features of User Datagram Protocol
else
if (Received_protocol ==Internet Control Message Protocol)
Infer features of Internet Control Message Protocol
2: After collecting the features wait for two seconds
3: Split the data into records based on the connection between two Internet Protocol addresses.
4: For all connection
Apply DT rules
5: Output of Log
6: End

4 Results and Discussion

In order to measure the performance of our proposed approach, a sequence of experiments on extracted dataset were conducted based on the following configuration. Our proposed method was implemented in Windows 7, Intel Pentium(R), CPU G2020, and Processer speed 2.90 GHz.

Table 1 presents the identification of the intrusion over several existing techniques with honey pot, and the result shows that the honey pot detection rate is high among them. There are total 12 features used, and in all features, the overall intrusion detection rate is high for the honey pot.

The intrusion detection shown in Fig. 2 is high in the honey pot techniques. When compared to existing techniques, the honey pot is most effective and efficient.

In Fig. 3, the result of the experiment presents the difference between Honey pot and some existing technique which is producing the irrelevant information to the

Table 1 Classifier and accuracy beyond intrusion

Features used	Classifier	Accuracy	Normal		DoS	
			True Positive	False Positive	True Positive	False Positive
12	OneR	82.625	0.895	1.001	0.811	0.213
12	C4.5	91.795	0.937	0.106	0.876	0.118
12	Naive bayes	81.443	0.854	0.059	0.806	0.105
12	Honey pot	97.953	0.999	0.003	0.979	0.001

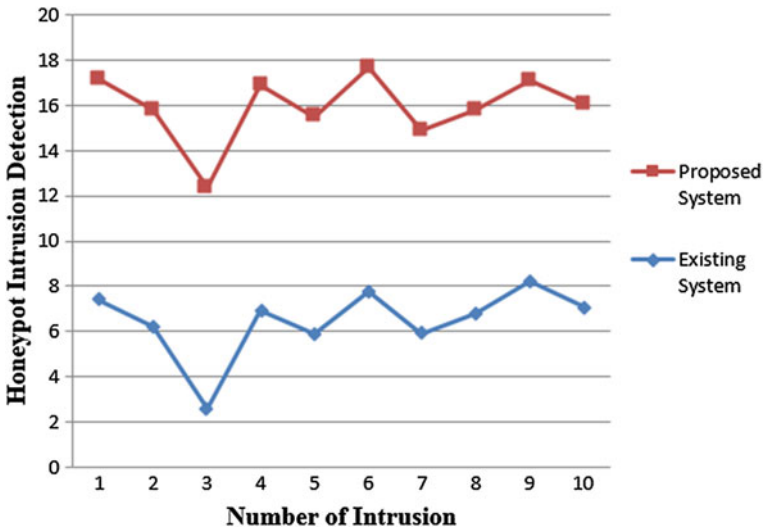

Fig. 2 Honey pot intrusion detection

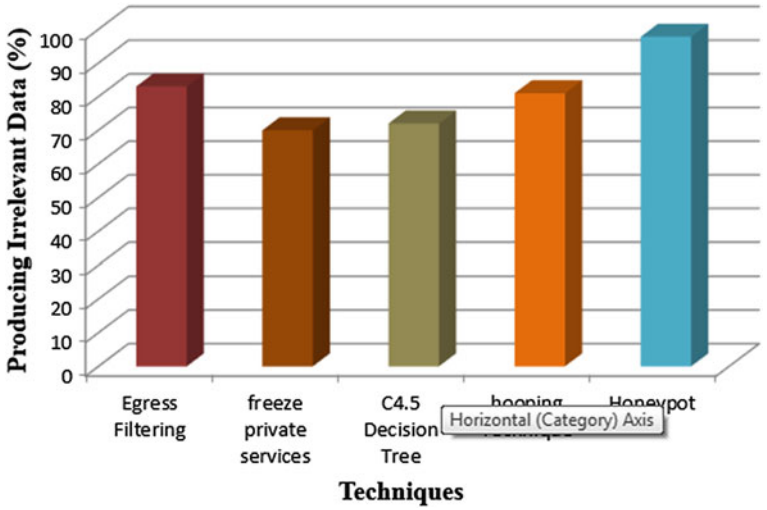

Fig. 3 Producing irrelevant information to attacker

intruders or attackers. The honey pot is producing the more irrelevant information to intruders or attackers, and it is one of the best techniques to gain the information about them.

5 Conclusion

In our proposed work, we have proposed a novel technique with the honey pot and IDS. These techniques are a major part for the defensive operations. These methods are very efficient for the security purposes on the network and prevent the stealing of data from the attackers or intruders. The proposed technique has main goal to confuse the intruders and collect their information in the system and show them a wrong path or send them to an irrelevant data. These techniques will help to identify the next move of the attackers with the novel ideas and technology. The attackers belong to the black-hat community, and they tends to steal the data from any system with a new techniques, so the obtaining information like IP address, TCP Address, etc., will surely help to know their further moves. By knowing attackers next move, honey pot will secure the users' information and prevent the intruder access on the network or system. The Honey pot system is playing a crucial role in detecting the attackers and showing them a fake database.

References

1. Shyamasundar, L.B.: An auto configurated hybrid honeypot for improving security in computer systems. Int. J. Comput. Sci. Inform. Technol. **6**(1), 84–88 (2015)
2. Parimala, H.C., Kavitha, B.: Achieving higher network security by preventing DDoS attack using honeypot. Int. J. Comput. Netw. Secur. **6**(1), 40–45 (2014)
3. Suruchi, N., Sandeep, K.: Advanced honeypot system for analysing network security. Int. J. Curr. Res. Acad. Rev. **2**(4), 65–70 (2014)
4. Fatih, H., Abdulkadir, P., Erkam, U., Bakır, Emre., Necati, S.: An automated bot detection system through honeypots for large-scale. In: 6th International Conference on Cyber Conflict, Estonia, pp. 255–272 (2014)
5. Meghana, S., Vidya, D.: Intrusion detection technique using data mining approach: survey. Int. J. Innov. Res. Comput. Commun. Eng. **2**(11), 6352–6359 (2014)
6. Brijendra, P., Ramakrishna, C., Rakesh, S., Sanjeev, K.: Implementation of port density based dynamic clustering algorithm on honey net data. Int. J. Adv. Comput. Eng. Netw. **2**(6), 76–82 (2014)
7. Dasen, R., Juan., W., and Qiren, Y.: An intrusion detection algorithm based on decision tree technology. In: Asia-Pacific Conference on Information Processing, Shenzhen, pp. 333–335 (2009)
8. McHugh, J., Christie, A., Allen, J.: Defending yourself: the role of intrusion detection system. IEEE **17**(5), 42–51 (2000)
9. Jeremy, B., Jean-Francois, L., Christian, T.: Security and results of a large-scale high-interaction honeypot. J. Comput. **4**(5), 395–404 (2009)
10. Das, V.: Honeypot scheme for distributed denial-of-service attack. In: International Conference on Advanced Computer Control, India, pp. 497–501 (2009)
11. Kuthadi, V.M., Rajendra, C., Selvaraj, R.: A study of security challenges in wireless sensor networks. JATIT **20**(1), 39–44 (2010)
12. Divya, A.C.: GHIDS: A Hybrid Honeypot System Using Genetic Algorithm. Int. J. Comput. Technol. Appl. **3**(1), 187–191 (2012)
13. Yun, Y., Hongli, Y.: Design of distributed honeypot system based on intrusion tracking. In: 3rd International Conference on Communication Software and Networks, China, pp. 196–198 (2011)
14. Jiqiang, Z., Keqi, W.: Design and implementation of dynamic virtual network. In: International Conference on Electronic and Mechanical Engineering and Information Technology, Harbin, China, pp. 2131–2134 (2011)
15. Selvaraj, R., Kuthadi, V.M., Marwala, T.: An effective ODAIDS-HPs approach for preventing, detecting and responding to DDoS attacks. Brit. J. Appl. Sci. Technol. **5**(5), 500–509 (2015)
16. Siva, T., Phalguna, K.E.S.: Controlling various network based ADoS attacks in cloud computing environment: by using port hopping technique. Int. J. Eng. Trends Technol. **4**(5), 2099–2104 (2013)