Buckler: Intrusion Detection and Prevention using Honeypot

Pagar Harshali Yashwant[1], Pathare Anjali Sanjay[2], Shaikh Sameer Shekhanur[3]
[1,2,3]*Student, Department of Computer Engineering, ATC Faculty of Engineering, Ahemadnagar, India*

***Abstract*: Recently, as result of dramatic connectivity between devices from a computer to mobile systems, security of information and availability of the services become more and more challenging. Internet usage is growing daily the world is coming closer making it a smaller place to live for its users. However, it has also managed to create problems for people because of the increase in cyber-crimes. So there is a need for monitoring and analyzing both user and system activities and thus tracking as well as blocking the malware is a must. This is where intrusion detection system (IDS) and intrusion prevention system (IPS) comes into the picture. One of the most efficient methods to stop network attacks is using IDS/IPS Systems. The ultimate goal of an IDPS system is to stop security attacks before they have been carried successfully. To detect or prevent network attacks, a network intrusion detection (NID) system may be equipped with machine learning algorithms to achieve better accuracy and faster detection speed. The majority of intrusion prevention systems use the detection methods which include Signature-based, Statistical anomaly-based and Honey pot based. Using these detection methods, the malware is detected, and then further actions are taken to block the malware. IPS techniques differ in how they scan the data streams to detect a threat or intrusion. Data capture and data control are used by the research community to study issues in network security, such as Internet worms, spam control, and Denial of Service (DoS) attacks. In this paper, we will be focusing on prevention from the various types of attack.**

***Keywords*: Intrusion detection system (IDS), Intrusion prevention system (IPS), Honeypot, Buckler, Denial of service (Dos), Net-work Security.**

1. Introduction

According to Steward Kirkpatrick et al. [1]. “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.”

It is thus, clear from this quote that with time as the web is evolving, systems no longer tend to remain safe i.e. there is always a constant threat to our data. Hence, we need a setup for the computers that can detect and prevent the different kinds of attacks that take place daily on the internet. Data is the major component of a network. Thus, its transmission, analysis, processing and usage has to be safe across the network, the system, therefore, is required to maintain a high degree of security.

The current system deals with honeypot based intrusion detection system which only detects whether an attack has taken place or not. Once the malware has been detected, no further actions are taken by the current IDS system.

In the existing system [3]-[6], the detection of attack is the primary purpose of the IDS System, which leaves it exposed to the threats of the attackers making it vulnerable. Thus it needs to be ensured that security of user data is the prime concern and appropriate measures need to be taken upon detection of each attack.

Our proposed idea stands to design a system that will the user’s activity and will recognize the pattern in the usage. Frequent malicious actions will attract an action from the IPS which can result in blocking of the system (in case the system proves to be extremely malicious). Also, the attack kind is prioritized depending on fatality and system's ability to recover from the attacks. System and close to near fatality receive the highest priority, such kinds of attacks, if initiated will lead to immediate suspension and blockage of the system from where the attack was originated.

Some attacks that are less malicious as compared to the highest one will be monitored accordingly. The spike in the frequency of this kind of attack will require the user to mention their unique ID and their passport image that will enable them to carry on further communication in the network.

In simpler words, our work is to make the systems secure against maximum kinds of attacks to protect users and their data.

2. Literature survey

N. Wattanapongsakorn, et al., 2013 have developed an IDPS System that is capable of classifying the different types of network attacks (i.e. DoS, Probe and internet worms) based on features of network packets. The system works on two operation modes: standalone and distributed. In standalone mode, the system resides on the gateway and the traffic is monitored only by a single system while in distributed mode, the sniffers are in different points capturing packets. The malicious packets are processed, classified and finally blocked by protection part using iptables.

An intrusion detection system was realized by Rowayda A.Sadek which uses neural networks and two other algorithms acting on NSL-KDD database for a better selection of attributes. He showed against six other research that his algorithm is more efficient in detecting rate 96.7% and the number of false positive that is generated 3.0%.

Yong-Ho kim et al. have propositioned a fashion of calculating the likelihood of Advanced Persistent Threat (APT) centered around Intrusion Detection Event (IDE) and an efficient relationship to realize and asses the IDE through a novel idea of segmenting the testing into period of Learning , Prediction and Evaluation. A set of well-crafted features have been selected to make the prediction as accurate as possible.

The proposed model collects and pre-treats IDE to identify cyclical patterns and converges them into a single IDE. It also mines data concerning threads and sessions to categorize them into unidirectional and bi-directional interventions amongst source and target locale. The model also builds attack scenarios to isolate the framework of attack. Finally, the model predicts intrusions events by evaluating the context of previous attacks.

3. Proposed architecture

A. System diagram

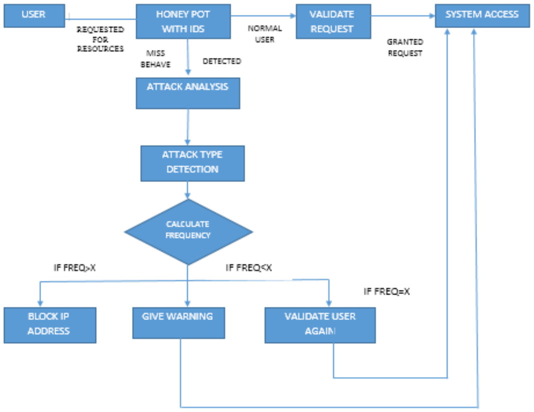

Fig. 1. Proposed system architecture

The above diagram showcases the proposed architecture. It is divided into two sections.

1) Honeypot

Considering the classical field of computer security, a computer needs to be secure, but in the domain of Honeypots, the security holes are set to open on purpose. Honeypots can be defined as a trap which is set to detect attempts at any unauthorized use of information systems. Honeypots essentially turn on the tables for Hackers and computer security experts. The main purpose of a Honeypot is to detect and learn from the attacks and further use the information to improve security. Honeypots have long been used to track attackers' activity and defend against coming threats. There are two types of honeypots:

1. Research Honeypot: A Research Honeypot is used to study about the tactics and techniques of the intruders. It is used as a watch post to see how an attacker is working when compromising a system.
2. Production Honeypot: These are primarily used for detection and to protect organizations. The main purpose of a production honeypot is to help mitigate risk in an organization.

Table 1
List of attacks supported by buckler

Category	Attack	Description
Category 1	Password-Based Attacks	Gain access rights to a network resource by hacking a valid user account
Category 1	IP Spoofing	Access network with a valid IP address and then modify, reroute or delete data.
Category 1	Application Layer Attack	Targeting application layer and gaining control over it.
Category 1	Compromised Key Attack	Obtaining the key to Obtain access to a secured communication
Category 1	Sniffer Attack	An application that can read, monitor, and capture network data exchanges and read network packets
Category 2	Data Modification	Modify Data without the knowledge of sender or receiver
Category 2	D-DoS (Distributed Denial of Service)	Prevent legitimate users from accessing services or information
Category 2	Brute Force	Decoding a password using trial and error
Category 2	SQL Injection	Embedding malicious code in a poorly-designed application and then passed to backend database
Category 2	SSL (Secure Sockets Layer) Attacks	Intercept the encrypted data before it can be encrypted, giving the attacker access to sensitive data.
Category 3	DNS Attack	Redirecting users to a bogus website when they are trying to access a legitimate one.
Category 3	Cookie Poisoning	Examining and editing the cookies stored to get secured information
Category 3	Cross-site Scripting	Enables attackers to inject client-side scripts into web pages viewed by other users.
Category 3	Drive-by-Downloads	A user downloading content without understanding the consequences caused by it
Category 3	Malvertising	Injecting malicious advertisements into legitimate networks
Category 4	Future and Heuristic Attacks	Attacks with no probable solutions or which have not been discovered yet.

2) Buckler (Intrusion Prevention System):

In this, 'Buckler' comes into picture when any attack is detected. Attacks detected are classified into four types according to their priority. The attacks with the highest priority come under Category 1 which are very harmful to the system and need to be taken care of immediately. So as soon as the attack is encountered, that is, the frequency is 1, Buckler (Intrusion Prevention System) blocks the IP address of the user, and consequently the request is not validated. Hence the system will not permit the IP address to make any further request.

Attacks with less priority are placed in category 2 and category three respectively. These attacks are not very detrimental, and so their effect on the system is less damaging. There is a predefined limit set up to which the system does not get affected and remains intact. Moreover, if the frequency of attacks is less than the preset threshold, a warning is sent to the system, and if the rate exceeds the limit, the user is requested to submit their UID (unique identity) and to upload their passport for verification. After successful verification, the user is granted access to the system. In Category 4, all the attacks that have not been discovered, or the attacks that have no probable solution are placed. Hence, by the use of Buckler, one can secure the system's privacy and protect it from all the Trojans, malware and vulnerabilities that can harm the system. Therefore, our proposed architecture helps to not only detect but also combat the attacks on a system.

B. Use case Diagram

Use Case Diagram. Example is given below It shows a set of use cases and actors (a special kind of class and their relationship).Use case diagrams address the static use case view of system. These diagrams are especially important in organizing and modeling the behavior of a system.

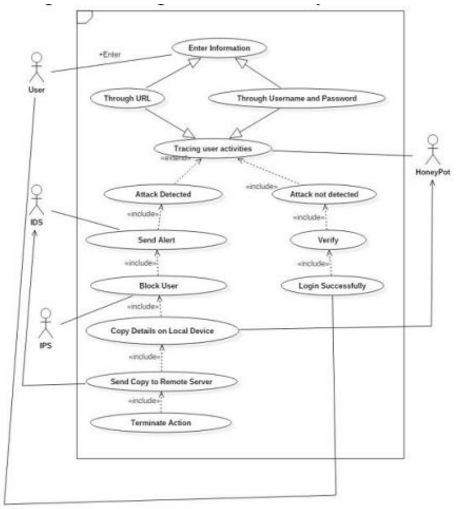

Fig. 2. Use case diagram of buckler system

4. Feasibility status

All projects are feasible, given unlimited resources and infinite time. But the development of software is plagued by the scarcity of resources and difficult delivery rates. It is prudent to evaluate the feasibility of the project at the earliest possible time.
Three key considerations are involved in feasibility analysis.

A. Economic feasibility

This procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. It benefits outweigh costs, and then the decision is made to design and implement the system. Otherwise, further justification or alternations in proposed system will have to be done if it is to have a chance of being approved. This is an ongoing effort that improves in accuracy at each phase of the system lifecycle.

B. Technical feasibility

Technical feasibility centers on the existing computer system (Hardware, Software, etc.,) and to what extent it can support the proposed addition. If the budget is a serious constraint, then the project is judged not feasible. The project needs extensive research and the internet based technologies are expanding by the day, it gives rise to much larger and the variety of attacks on a network.

C. Operational feasibility

People are inherently resistant to change, and computers have been known to facilitate change. It is understandable that the introduction of a candidate system requires special effort to educate, sell, and train the staff on new ways of conducting business.

5. Outcome

The outcome of the project is:

1. Collect Real Data: While Honeypots collect a small volume of data but almost all of this data is a real attack or unauthorized activity.
2. Reduced False Positive: With most detection technologies (IDS, IPS) a large fraction of alerts is false warnings, while with Honeypots this doesnt hold true.
3. Cost Effective: Honeypot just interacts with malicious activity and does not require high-performance resource.
4. Encryption: With a honeypot, it doesnt matter if an attacker is using encryption; the activity will still be captured.
5. Simple: Honeypots are very simple to understand, deploy and maintain.

6. Summary and conclusion

Our proposed Honeypot based Intrusion Detection System has significantly improved detection rate of Intrusion Detection System and drastically reduce false positives hence enhances the overall efficiency of the Intrusion Detection System. Honeypot based Intrusion Detection System has significantly Increased Average Throughput and Packet Delivery Ratio. Proposed System has remarkably reduced Energy Spent and Packet Drop Rate. All above parameter shows better efficiency of the Honeypot Based Intrusion Detection System. However Jitter is not reduced which is undesired. Further our proposed system can be coupled with other Intrusion Detection Systems to enhance their capabilities and overall efficiency of our proposed system.

References

[1] Intrusion Prevention, http://searchsecurity.techtarget.com/definition/intrusion-prevention/,
[2] IPS, https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips
[3] Prathamesh P Churi, Shreya Bondre and Neha Gavankar. Honey patterns: Recognizing Pattern based Attacks on Websites. International Journal of Computer Applications 161(9):8-11, March 2017
[4] Xiangfeng Suo, Xue Han and Yunhui Gao, "Research on the application of honeypot technology in intrusion detection system,"2014 IEEE

Workshop on Advanced Research and Technology in Industry Applications (WARTIA), Ottawa, ON, 2014,pp. 1030-1032.

[5] Dongxia, L. and Yongbo, Z., 2012, March. An intrusion detection system based on honeypot technology. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 451-454). IEEE.

[6] Chakraborty, N., 2013. Intrusion detection system and intrusion prevention system: A comparative study. International Journal of Computing and Business Research (IJCBR), 4(2), pp.1-8.

[7] Pomsathit, A., 2012, May. Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Honeypot. In Engineering and Technology (S-CET), 2012 Spring Congress on (pp. 1-4). IEEE.

[8] Petrunić, A.R., 2015, May. Honeytokens as active defense. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on (pp. 1313-1317). IEEE.

[9] Yin, C., Li, M., Ma, J. and Sun, J., 2004, May. Honeypot and scan detection in intrusion detection system. In Electrical and Computer Engineering, 2004. Canadian Conference on (Vol. 2, pp. 1107-1110). IEEE.

[10] Yang, Y. and Mi, J., 2010, April. Design and implementation of distributed intrusion detection system based on honeypot. In Computer Engineering and Technology (ICCET), 2010 2nd International Conference on (Vol. 6, pp. V6-260). IEEE.

[11] Qbea'h, M., Alshraideh, M. and Sabri, K.E., 2016, August. Detecting and Preventing SQL Injection Attacks: A Formal Approach. In Cybersecurity and Cyberforensics Conference (CCC), 2016 (pp. 123-129). IEEE.

[12] Chowdhary, M., Suri, S. and Bhutani, M., 2014. Comparative study of intrusion detection system. International Journal of Computer Sciences and Engineering, 2(4), pp.197-200.

[13] Wondracek, G., Holz, T.,Kirda,E.and Kruegel,C.,2010, May. A practical attack to de-anonymize social network users. In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 223-238). IEEE.

[14] Tang, Y., Hu, H., Lu, X. and Wang, J., 2006, April. Honids: Enhancing honeypot system with intrusion detection models. In Information Assurance, 2006. IWIA 2006. Fourth IEEE International Workshop on (pp. 9). IEEE.