International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Advance Honeypot Mechanism- The Hybrid Solution for Enhancing Computer System Security with DoS

Swapnali Sundar Sadamate[1], V. S. Nandedkar[2]

[1]Pune University, PVPIT College, Student of Department of Computer Engineering, Bavdhan, Pune-21, India

[2] Pune University, PVPIT College, Professor of Department of Computer Engineering, Bavdhan, Pune-21, India

Abstract: ***Computer system security is one of the most popular and the fastest evolving Information Technology (IT) in organization. Protection of information access, availability and data integrity represents the basic security characteristics desired on information sources. Any disruption of these properties would result in system intrusion and the related security risk. Advanced decoy based technology called Honeypot has a huge potential for the security community and can achieve several goals of other security technologies, which makes it almost universal.This topic is devoted to sophisticated hybrid Honeypot with autonomous feature that allows to, based on the collected system parameters, adapt to the system of deployment. By its presence Honeypot attracts attacker by simulating vulnerabilities and poor security. After initiation of interaction Honeypot will record all attacker activities and after data analysis allows improving security in computer systems. Also this paper contains techniques in a hybrid combination of detection of DOS and different attack types by using naive's classification algorithm.***

Keywords: Honeypot, Packet Capturing, IDS, DOS.

1. Introduction

Computer security is among one of the main areas of information technology. Over recent years mentioned area achieves the biggest progress because nobody wants that exactly his system will be attacked and intruder or anybody else will receive the stolen data. Whichever more experienced attacker can exploit weaknesses in the security system and penetrate through its defense mechanism to obtain sensitive data. It's necessary to put high priority to system security, minimize vulnerabilities and secure the computer system against intrusion.

The interaction with intruders will decoy based equipment start to gather detailed information which are necessary for elimination system security holes. This advanced decoy based technology is called "Honeypot". Suggested solution includes a unique sophisticated autonomous characteristic that allows deployment in any environment and allows auto configuration process based on the collected parameters about the current environment thorough passive fingerprinting method. Subsequent chapters contain a description of the security system using IDS in combination with Honeypot technology with autonomous ability of detecting different attack types by naïve bays classifier with DOS attack detection

2. System Architecture

System architecture of our solution contains client-server architecture.

2.1 Server Architecture

Due to centralization of data collected at the same time the main Server is connected to multiple customers and that knowledge are all stored in the database is set up to receive incoming message. The attackers intended to reconcile the different reports indicated with the computer system areas to attack massive attack or full-range scanning purposes. The three main parts, which are the data normalized database to stored prior to proposed server architecture are**:**

- Sebek server – at the same time receives and filters several data sources representing instructions or a connection to incoming data storing process.
- Dionaea server – accepts patterns of malicious code that sends the dionaea client part.
- Verification process – a modular scheme of hybrid open-source system for intrusion detection. It's using standard communication format. It can be adapted to the needs of an extensive system from any point of deployment, receives the amount of data from clients and integrates diversified data formats.
- Web-server interface displays all information about captured attack. In case of abnormal circumstances are specific messages highlighted through the web interface for in time response.

2.2 Client Architecture

Because of gathering data about attacker activities during an attack are installed clients placed in the same domain. Various parts of the system are independently activated for collecting set of data depending on attack type. Obtained data are subsequently backward delivered to a server to facilitate

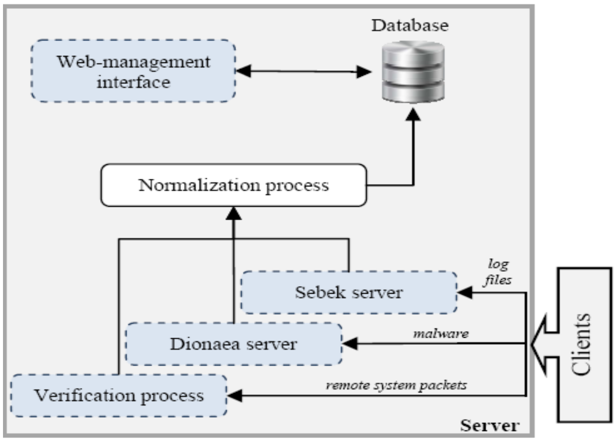


Figure 2.1: Server architecture

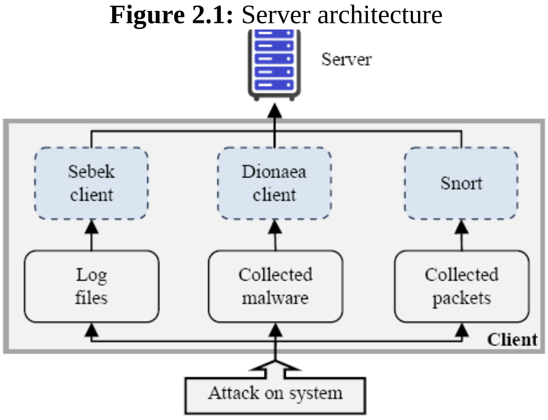


Figure 2.2: Client architecture

further analysis and for the subsequent updating system security. Client architecture (Figure 2.2) consists of three components/tools:

- Sebek client – records attacker behavior during interaction with the Honeypots in log files.
- Dionaea client – attracts attackers and captures the patterns of malware by simulating basic system services and vulnerabilities.
- Snort – monitors and filters packets during detecting intrusions. It Identifies patterns of separate attacks, information and warning messages.

The most ideal solution provides usage of proposed autonomous sophisticated Honeypot concept for detection process.

2.3 Algorithm of Proposed System

2.3.1 Bayes Classifiers

Algorithm of Proposed System Using Bayes Classifiers	
Input: Different attributes of packets	
Step 1	p(cj|d) = probability of instance d being in class cj, This is what we are trying to compute
Step 2	p(d|cj) = probability of generating instance d given class cj, We can imagine that being in class cj, causes you to have feature d with some probability
Step 3	p(cj)= probability of occurrence of class cj This is just how frequent the class cj, is in our database
Step 4	p(d)= probability of instance d occurring which says p(cj |d) =p(d| cj)p(j)/p(d)
Output: Variance in attributes in terms of time	

Assume that we have two classes :

c1=ruleset, and c2=attack.

p(d) = attacks occuring in the system according to rules...(snort ruleset we have added)

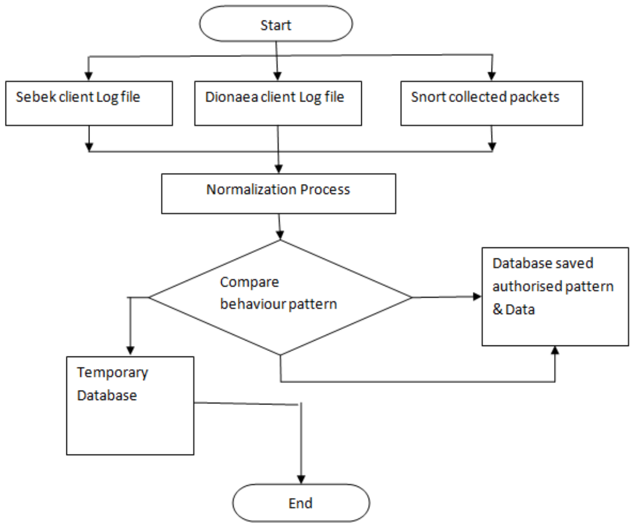
We are going to detect the attacks in the system we do not know how many attacks are present in the system and what are the types of attacks are there. Classifying this attack as per the ruleset is the main aim of this classifier and it also detects the attacks in the system.

2.3.2 Detection Mechanism for DOS

In this section, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a predetermined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record.

Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low-quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle-area-based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

3. System Design



4. Result Analysis

4.1 Existing System

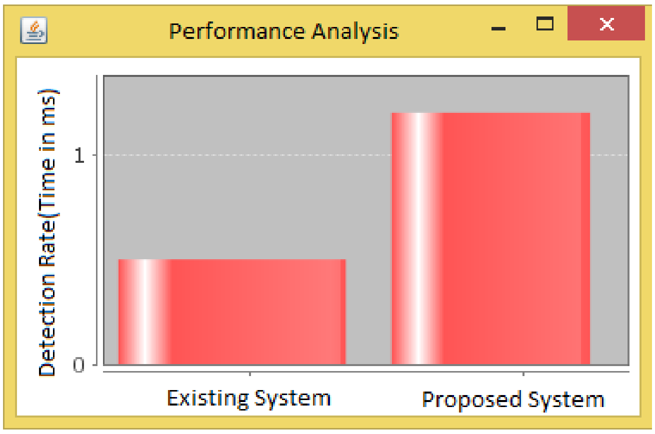
Traditionally oriented approach to security is largely focuses on defense. Due to the growing amount of attacks the more aggressive form of defense comes to the fore. Booby traps equipment's which are simulating the most often system weaknesses and unsecured system services attract potential attackers, with their presence in target system, to start attack. Honeypot consists of a combination of security tools: Snort

IDS, Sebek and Dionaea. Tools were selected based on their properties analyzed above. The detection mechanism based on a sophisticated hybrid Honeypot integrated in the client-server architecture consisting of centralized main server and multiple client stations. Client workstations serve to capture suspicious activity or directly record the malicious code which is then send to server for processing. Server analyzes received data, decides to issue or not to issue a security warning and displays cumulative information through a web interface.

4.2 Proposed System

An advantage of the naive Bayes classifier is that it requires a small amount of training data to estimate the parameters (means and variances of the variables) necessary for classification. Because independent variables are assumed, only the variances of the variables for each class need to be determined and not the entire covariance matrix.

4.3 Performance Analysis Graph



Graph between existing and proposed system

5. Conclusion

Honeypots becoming highly flexible solution, Not only their deployment and management become more cost-effective, but also provide a much better integration into the system, thereby minimizing the risk of human error during manual configuration. Merger with the surrounding system in addition minimizes the risk of identification by attackers. Just as all new technology, the decoys also have some shortcomings that need to be overcome and eliminated. Honeypot is excellent security tool but it is not a panacea for a securing the whole system. The apart of this work is improving the IDS detection mechanism and minimizing the number of generated false positives and also false negatives using advanced technology called Honeypot.

The work includes proposal of an autonomous special safety feature by using KNN algorithm for detecting attack type and by using SVM for intrusion detection for enhancing security of distributed computer systems. Unique proposal combines a variety of security tools, to order to minimize their disadvantages and maximize the security capabilities in the process of intrusion detection. Triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.

References

[1] J. McHugh, A. Christie, J. Allen, “Defending Yourself: The Role of Intrusion Detection System,” IEEE Software, IEEE Computer Society, pp. 42-51, October 2000.

[2] R. Chandran, S. Pakala, “Simulating Network with Honeyd,”[online], Technical Paper, Paladion Networks, December 2003.Available on:<http://www.paladion.net/papers/simulating_networks_with_honeyd.pdf>.

[3] F. G. Lyon, “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,” [online], Nmap Project, USA, ISBN 978-0979958717, January 2009. Available on: <http://nmap.org/book>.

[4] L. Vokorokos, A. Baláž, “Host-based Intrusion Detection System,“ IEEE 14th International Conference on Intelligent Engineering Systems, Budapest, pp. 43-47, ISBN 978-1-4244-7651-0, 2010.

[5] L. Spitzner, “The Value of Honeypots, Part One: Definitions and Values of Honeypots,” Security Focus, 2001.

[6] L. Spitzner, “Honeypots: Tracking Hackers,” Boston, USA: Addison-Wesley, Parson Education, ISBN 0 321-10895-7, 2003.

[7] S. Karthik, B Samudrala, A. T. Yang, “Design of Network Security Projects Using Honeypots,” Journal of Computing Scienes in Colleges, 2004.

[8] R. Baumann, C. Plattner, “White Paper: Honeypots,” Swiss Federal Institute of Technology, Zurich, 2002.

[9] N. Provos, “Developments of the Honeyd Virtual Honeypot,”[online]. Available on: <http://www.honeyd.org>.

[10] A. Baláž, N. Ádám, “Intrusion Detection System Using Multilayer Perceptron,” 6th PhD Student Conference and Scientific and Technical Competition of Students of FEI Technical University of Košice, pp. 13-14, ISBN 8080860351, 2006.

[11] Snort[online].Available on: <http://www.snort.org>.

[12] Sebek[online].Available on:<http://www.honeynet.org/tools/sebek/>.

[13] Dionaea catches bug [online]. Available on: <http://dionaea.carnivore.it/>.

[14] E. Danková et al., “An Anomaly-Based Intrusion Detection System,” Electrical Engineering and Informatics 2, Košice, ISBN 978-80-553-0611-7, 2011.

[15] Securing WMN using hybrid honeypot system Author(S)Rawat, Paramjeet; Goel, Sakshi; Agarwal, Megha; Singh, Ruby PUB. DATEMay 2012 SOURCEInternational Journal of Distributed & Parallel Systems;May2012, Vol. 3 Issue 3, p29.

[16] Distributed web honeypots, Ryan Barnett,Christian Bockermann (http://www.jwall.org), Lukasz Juszczyk (CERT Polska), Josh Zlatin (Pure Hacking), Tony Carter (iTrustlabs), Steeve Barbeau. 2013.

[17] A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis, Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE,