International Journal of Education, Science, Technology and Engineering
p-ISSN: 2685-1458, e-ISSN: 2684-9844

Original Research Paper

HONEYPOT: Intrusion Detection System

Akshat Divya[1*], Anchit Bhushan[1], Nihal Anand[1], Rishabh Khemka[1], Sumithra Devi K. A[1]

[1] *Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India.*

Article History
Received:
03.03.2020

Revised:
02.04.2020

Accepted:
23.04.2020

***Corresponding Author:**
Akshat Divya
Email:
akshatdivya@hotmail.com

Abstract: The number of computers connecting to the internet is getting increased day by day, while the number of computers connected is increasing then it is obvious that the amount of network-based attacks will also increase. In this way, we use a honeypot that is a framework trap that is set to act against unapproved utilization of PCs and data frameworks. Around the globe, a huge number of individuals get to the web each day, honeypot which can likewise be called Intrusion Detection Technology is another time of security innovation that screens device to avoid malicious sports. The whole factor of this research paper is an Intrusion Detection System and Intrusion Prevention System, elements accomplished via honeypot and honeytrap methodologies. A great deal of research went into this review paper and the discoveries propose that the honeypots are drawing in light of a legitimate concern for analysts as a significant security system that can be actualized to stop or occupy the assaults the system assaults and give a chance to find out increasingly more about the source and nature of these assaults. Hence we can say that a honeypot can be utilized as an examination apparatus to accumulate increasingly more data about the expanding number of system assaults that are going on consistently.

Keywords: Intrusion Detection System, Honeypot, Hackers, Malicious, Attackers.

1. Introduction

The quantity of gadgets associated with the system is expanding step by step which brings about the expansion of system based assaults. A honeypot in this examination can be seen as a resistance mechanism that will monitor suspicious activity and will also keep a record of such activities. Today everybody is associated with a system whether it is through a PC or a portable device. Therefore something should be there to prevent these devices to fall prey to such network attacks. Honeypot does exactly this and acts as a wall between the threat and the user. Many important things happen on the network such as data exchange, transactions, etc. These exchanges include the enormous entirety of assets being moved. Regardless of how little the exchanges are they are should have been conveyed in a protected situation. If we use a honeypot as a safety feature then firstly, the attacker will actually be diverted to these honeypots instead of harming the actual transaction and hence with the help of honeypot we can get the details of the attacker as well. Secondly, we can use the data gathered by the honeypot and use that particular data to build an even better defense system.

The purpose of this paper is to give an examination respect to the examples and headway of honeypot for various authorities investigating at this moment. The paper contains the usage, advantages and implementation of honeypots and will be helpful to anyone in the future if they wish to research in the network security domain. [1]

2. NSL-KDD Dataset

With the continued growth of the interconnected computer, it also suffers various vulnerabilities. The studies on these vulnerabilities are primarily based on various Machine Learning techniques on the KDD dataset. Finding the answer as we take a look at the NSL-KDD dataset for finding accuracy in intrusion detection.

Table 1. NSL-KDD Dataset

Features	**Features**
duration	is_guest_login
protocol_type	Count
service	srv_count
flag	serror_rate
src_bytes	srv_serror_rate
dst_bytes	rerror_rate
land	srv_rerror_rate
wrong_fragment	same_srv_rate
urgent	diff_srv_rate
hot	srv_diff_host_rate
num_failed_logins	dst_host_count
logged_in	dst_host_srv_count
num_compromised	dst_host_same_srv_rate

3. Implementation

In this research the existing methodologies of implementing a honeypot led us to arrive at a much more reliable way of authenticating users and thus restricting the access of unauthorized users from entering into the system.

4. Methodology

4.1. Roaming Honeypot and Backpropagation

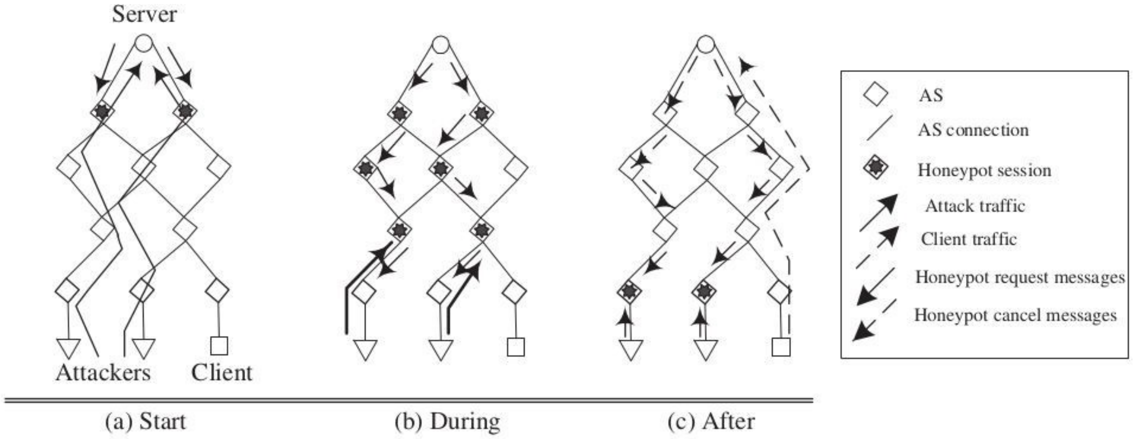
What this scheme is that it lets in fork out of N servers to be simultaneously active, whereas the closing N-K acts as a honeypot. The area of present-day lively honeypots is modified randomly. But the statistics about the change are shared most effective to the servers and the legitimate customers. Therefore the valid customers are cautioned to send their request to best the lively servers. The attack requests can be redirected to the honeypot.

The supply copes with any request that hits the honeypot is blacklisted. Now the blacklisted requests will be processed and details will be extracted about the attacker and by doing this we ensure that all future requests are rejected from that source address.

The backpropagation algorithm is joined with the Roaming honeypot scheme to protect against source-address parodying DDoS assaults. In this method, the source address of the suspicious packet is traced back to its original source and filters are installed as near as it can be to the source of the intrusion [2. 3].

Inter-AS Propagation

In Inter-AS Propagation, while the honeypot ages, back-propagating honeypot meetings are made in the Autonomous System (AS's) upstream of the server towards the assault source. In a particular AS, If a packet getting into an AS is destined for the identical assault server the, honeypot periods are in addition created in the AS from which the packet changed into received. The returned-propagation stops if no more packets are obtained or non-transit AS is reached. A non-transit AS doesn't permit the float of bundles from various resources. HoneyPot periods then install filtering regulations in this non-transit ASs. All other honeypot sessions are destroyed at the cease of honeypot epochs [4].



(a) Start (b) During (c) After

Figure 1. Inter-AS Propagation

4.2. Ensemble Clustering

Whenever we are coping with unlabelled information, unsupervised anomaly detection is powerful. But with a false advantageous fee. Therefore we use the ensemble clustering approach to locate novel anomalies over the NSL-KDD dataset.

To grow the effectiveness of the NSL-KDD dataset there are some models that can be implemented.

- DBSCAN - It is a clustering method that is used to separate clusters of high density from clusters of low density.
- One-SVM - Traditional SVM classifier needs labeled records. In [5], the SVM classifier is adjusted into an unmonitored set of rules (One-SVM).
- Agglomerative Clustering - The agglomerative clustering is the most not unusual sort of hierarchical clustering used to group objects in clusters based totally on their similarity. It's also known as AGNES (Agglomerative Nesting).
- EM- Expectation–maximization (EM) algorithm is an iterative method to locate most probability or most a posteriori (MAP) estimates of parameters in statistical fashions, wherein the version depends on unobserved latent variables 6].

4.3. A Survey on Various IDS Techniques

The performance of various Algorithms is depicted in the table below with the advantages and disadvantages of each algorithm [7] – [11].

Table 2. Variuos IDS Techniques

Algorithm / Texhinique Used	**Reference Paper**	**Test Data Used**	**Purpose of IDS**	**Advantage**	**Limitation/ Future Scope**
Decisiion tree, random forest, K-NN	[2]	N/A	To accurantely detect potential attack	Produce impressive and efficient results in detecting IPV4-based attacks	IPV6 attack cannot be detected yet
Clustering and KDD	[3]	NSL-KDD 2009 dataset	To detect novel anomalies called NEC	Quality labelled datasets are not required	High false positive rate and high detection rate
Epigenetic algorithm	[8]	KDD-NSL	Additional information of future offspring	it helps to prevent more preciously the currable and not disseses based on environmental factors that do not fit in the sequenced gene	Reduction of total iterations to obtain the optimal splution is a shorter time
Genetic programming fuzzy inference system for classification (GPFIS-Class)	[11]	NSL-KDD	To solve problem of classification in IDS	Classification accurancy is higher	New GFS hybridised with a neural network

The information that can be drawn from the details stated above is the paper [8], has accuracy and detection price maximized to 90.12% whereas the techniques suggested by us boom the effectiveness and detection price up to 95%. A Survey from [3] consists of a high false effective price, however, our machine reduces the false high-quality price relatively [6].

4.4. Dynamic Honeypot

The above identity discusses the design of a dynamic honeypot, which can be described as a self-reliant honeypot that is capable of adapting in a dynamic and continuously converting community environment.

Dynamic configuration for honeypot is a milestone for this honeypot mechanism. To appropriately blend in with the environment, a honey pot should be designed which can mimic the production hosts inside the network environment which is extremely powerful.

Dynamic honeypot server begins by way of amassing information approximately the hosts available at the networks the use of the active or passive methods. The administrator has the selection of selecting the first-rate facts collecting method for use based totally on the community structure [7].

4.5. Honeynet

A honeynet is a combination of several types of honeypots working together in a cluster of the network. Every honeypot in a honeynet has its own characteristics implementing a specific security functionality. It is important to understand the fact that implementing a honeynet with homogeneous honeypots is easy but not of great importance. Thus it is necessary to implement a honeynet with a heterogeneous honeypot. Now to do that is not simple, it requires a framework that integrates all the honeypots involved in the honeynet.

Technology impartial honeynet description language (TIHDL) is a standard language designed to explain the honeynets. The versatility of Honeyvers is executed through two predominant competencies: first, it lets in the honeynet state of affairs to be described by TIHDL; Secondly, it accepts diverse current deployment platforms to be plugged in.

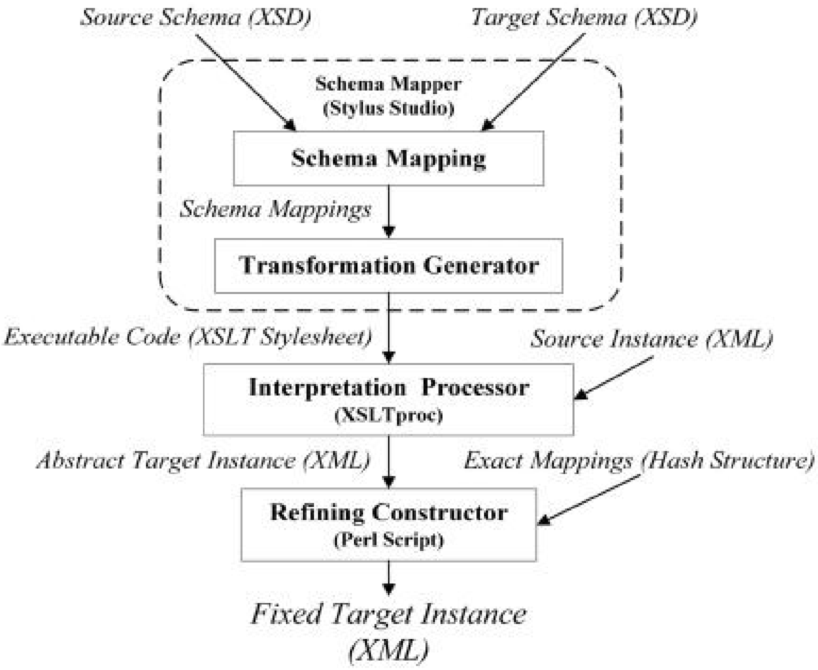


Figure 2. TIHDL Makes Use of XML-sytax

TIHDL makes use of XML-syntax, we observe the schema mapping methodology for information integration and transformation. The transformation method contains four steps. The venture at every step is executed through unique equipment [9].

5. Conclusion

This proposed honeypot which is based on Intrusion Detection System has notably progressed detection price of Intrusion Detection System and substantially lessens false positives, as a result, complements the overall efficiency of the Intrusion Detection System. Honeypot based Intrusion Detection System has substantially Increased Average Throughput and Packet Delivery Ratio. The proposed System has remarkably lowered Energy Spent and Packet Drop Rate. All the above parameters suggest a higher efficiency of the Honeypot Based Intrusion Detection System. However, Jitter isn't reduced which is undesired. In the near future, new and improved algorithms can be applied to reduce Jitter. Further, our proposed system may be coupled with other Intrusion Detection Systems to decorate their skills and ordinary performance of our proposed machine.

References

[1] K. R. Sekar, V. Gayathri, G. Anisha, K. S. Ravichandran, and R. Manikandan, “Dynamic Honeypot Configuration for Intrusion Detection,” in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)*, 2018.

[2] M. Anbar, R. Abdulah, I. H. Hasbullah, Y. C. Wey, and O. E. Elejla, “Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection,” in *the Annual Conference on Privacy Security and Trust (PCT)*, Penang, Malaysia, 2016.

[3] W. Chen, F. Kong, F. Mei, G. Yuan, and B. Li, “A novel unsupervised Anomaly detection Approach for Intrusion Detection System,” in *IEEE 3rd International Conference on big data security on cloud*, Zhejiang, China, 2017.

[4] S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mossé, and T. Znati, *Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks*: *Technical Report TR-04-111*. Department of Computer Science, University of Pittsburgh, 2004.

[5] W. Chen, F. Mei, F. Kong, G. Yuan, and B. Li, “A Novel Unsupervised Anomaly Detection Approach for Intrusion Detection System,” in *IEEE 3rd International Conference on Big Data Security on Cloud*, 2017.

[6] A. Borkar, A. Donode, and A. Kumari, “A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS),” in *the International Conference on Inventive Computing and Informatics (ICICI 2017)*, 2017.

[7] D. Fraunholz, M. Zimmermann, and H. D. Schotten, “An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy,” in *ICACT2017*, February 19-22, 2017.

[8] M. Ezzarii, H. Elghazi, H. E. Ghazi, and T. Sadiki, “Epigenetic Algorithm for Performing Intrusion Detection System,” in *2016 International Conference on ACOSIS*, Rabat, Morocco, October17-19, 2016.

[9] W. Fan, D. Fernández, and Z. Du, *Versatile Virtual Honeynet Management Framework*. The Institution of Engineering and Technology, 2016.

[10] A. L. Buczak, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, 2016.

[11] M. Belhor, and F. Jemili, “Intrusion Detection based on genetic fuzzy classification system,” in *IEEE 13th International Conference on Computer Systems and Application (AICCSA)*, Sousse, Tunisia, 2016.