www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-8, Issue-4, August 2020
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

E-ISSN:2321-3256

A Novel Based Approach to Detect and Take Action Against Network Intrusion in Virtual Machine Network System

Keesara.Sravanthi[1*], A. Srinivas[2], G. Narsing Rao[3], T. Raghu[4], P. Rakesh[5]

[1,2,3,4,5]Department of Information Technology, VNRVJIET, Hyderabad, India

**Corresponding Author: sravanthi_k@vnrvjiet.in*

Received: 17/Jun/2020, Accepted: 20/Aug/2020, Published: 31/Aug/2020

Abstract— The design of intrusion detection systems (IDS) has received significant attention in the field of computer sciences with the massive number of network traffic and security risk. While various methods and strategies have been proposed for tracking Client and company behaviour and analyzed together to detect network intrusion. As there is latent information on further research in the classification and clustering of network packet signatures. We propose that the system of intrusion detection based on network signatures and system studies should be supported in this article. We include a KDDCUPSET which is used to store different modes of attacks and a multi - phase detector to identify potential intruders more effectively and a text-based query generation framework to challenge the detector module's suspended requesters. If qualities of a received System Packet contest are certified, the classification alerts the admin to the potential precaution with the basis of cruel behavior and the classification must be above 90 percent accurate.

Keywords— Machine Learning algorithm, NIDS, Clustering, Packet signatures.

I. INTRODUCTION

Network security include of necessities as well as policies adopt by a system admin to circumvent and supervise unauthorized admission, abuse, variation of a system network and network-attainable assets. Network security involve the authorization of access to data in a network, which is restricted by the network admin. Users prefer or are assign an ID and password or new authenticate data that allow them admission to information and program in their ability. In past, hackers were extremely expert programmers who unstated the facts of computer communications and how to take advantage of vulnerabilities. At present approximately anyone can grow to be a hacker by downloading utensils from the Internet. These complex attack utensils, usually open networks have generated an improved call for network security and active security policies. The better approach to defend a network from an external attack is to secure it off entirely from the external world. Congested network provides connectivity only to trusted recognized parties and sites; a congested network does not let a connection to public networks. The significance of information comes from the characteristics it contains: Accessibility, Accuracy, Authorization, Privacy, Reliability, Value. [1] Network Attacks and Types Networks attacks are focus to attacks from malicious sources. Network attack is the intrusion or threat can be distinct as any purposeful act that attempt illegal access of Information management and by exploiting the accessible vulnerabilities in the system. A Network attack is purposeful management of mainframe systems, technology dependent enterprise and network. Network attacks exploit cruel system to modify PC system, reason or information, ensuing in troublemaking penalty so as to cooperate information and guide to cybercrimes, such as information and individuality stealing. Network intruder intercept data travelling throughout the network is known as passive attack. Ex: Wiretapping, port and idle Scanner. [2] Network intruder initiate instructions to interrupt the network's operation is known as active attack. Ex: DOS, Spoofing, SQL Injection, Cross-site Scripting.

An intentional challenge to penetrate a network and break the security of the network and thus breaking the privacy of the data present in the systems of the network. The one who tries to challenge such an act is called as an Intruder and the act can be termed as Network Intrusion. It is any place of actions that test to cooperate the dependability, privacy of a source. IDS (Intrusion Detection System) can be a part of installed software or a objective application that monitors network traffic in array to sense unnecessary act and actions such as criminal and malicious traffic, traffic that violate security guidelines, and traffic that violate tolerable use policy. [3] Many IDS utensils will also store up a detected episode in a log to be reviewed at a later on or will unite actions with further data to make decisions concerning policies or damage control. An IPS is a type of IDS that can avoid or stop unnecessary traffic. The IPS frequently logs such actions and associated information. Intrusion Prevention System (IPS) leave lone footstep advance and not simply identify attacks although attempt to avoid them as well. [4] Functions of Network Intrusion Detection System: 1. Monitor and analyze together client and organization actions. 2. Analyze organization configurations and vital defects. 3. Assess organization and case reliability. 4. Capability to identify pattern distinctive of attacks. 5. Study of irregular action pattern. 6. track consumer guidelines violation.

II. PROPOSED METHODOLOGY

In our proposed system we are performing different task in different modules. We are providing a multistage detection to more precisely detect the possible attackers and a text-based with question generation module to challenge the suspend requesters who are detected by the detection by the detection module. We introduced the system and evaluated the performance to show that our system works efficiently to mitigate the DDoS traffic from the Internet. In our system when client attack is stored at admin side. Admin performs Turing test for client by generating questions. We are using KDDCUPSET for storing types of attacks. The client packets go through the comparing of packets with defined packets and if new pattern is detected it is stored in KDDCUPSET for prohibiting further attacks by different clients. The client who attacked with new pattern id blocked after detecting new pattern. In KDDCUPSET we are storing predefined attacks for our testing. From that KDDCUPSET we are taking patterns for attacks. We can store new patterns in that KDDCUPSET. In this model we improved accuracy rate better than existing model it will give 98% of precision level on any public networks and classical machine learning applied on the Deep Neural Network(DNN)for calculating the accuracy and network traffic.. This is done with the help of python using Jupiter and machine learning algorithms.The results will alert the administrator .

The various steps in intrusion detection include:

- Data collecting
- Data interpretation
- Data translation
- Data verification
- Data monitoring
- Data transfer
- Data conformation
- Data verification

In this project, either current or new user data will be stored in the database as inputs provided by user.

A. Advantages:
They are practical were we having a high number of works stations since it monitors the network as a whole from a particular point deployment.

➢ They excel at detecting attacks in progress and even responding to blocking them.
➢ Monitors a number of hosts simultaneously – the NIDS uses a promiscuous mode, reviewing the network traffic that is received. Processes that can take place simultaneously, without affecting network performance since any packets are added on the network in the process.
➢ The ability to cover network inherent security holes associated with vulnerability to many types of attacks, particularly DoS, which cannot be detected using a common audit trail analysis approach-network traffic analysis is needed here.
➢ System resources are less consumed than in the case of audit trail processing.
➢ Possibility of detection of novel attacks as intrusion.
➢ Very few false alarm rate, simple algorithms.
➢ Easy creation of attack signature databases.

B. System Architecture:
The major objective of our plan is to defend server-side resources that are to make the clients a valid request and if the some malicious action is establish then it should be handled at the IDS side and not at the server side. In the logic we can also call our system as “The packet assessment system”. [5] The structural design of our structure is specifies the system archite Although the firewalls and dissimilar antivirus software’s are there several hackers can penetrate the firewall. [6] Hence network intrusion detection system (NIDS) knowledge is come into action. The intrusion detection system (NIDS) essentially analyzes and monitors the network behavior of a computer system as exposed in Figure. Depending on throughput necessities, a system-based IDS might study only packet headers or contain the information. Additionally, various detectors are naturally engaged at deliberate actions in order to issue the job.

- Virtual machine can be used to execute the structural design of multimodal based irregularity IDS with Network based IDS system.
- Then Packet investigation and testing can be made by using the training data sets.
- Categorization of the packets can be made by means of the regulations which distinguish the malicious and usual packets. With that it will notice the original attacks.
- To mark a Packet Capture Program using (JPCAP), to capture the real time network traffic.
- Captured packets features can be analyzed
- Designed to execute the multimodal based abnormality IDS with Network IDS algorithm using python code and build it to work with real packets.
- It is simple to adapt or restore any class with no disturbing other third parties.
- Separate device and database features ensure improved weight balancing.
- Sufficient security measures can be implemented inside third-party servers without hindering clients. cture of the system.

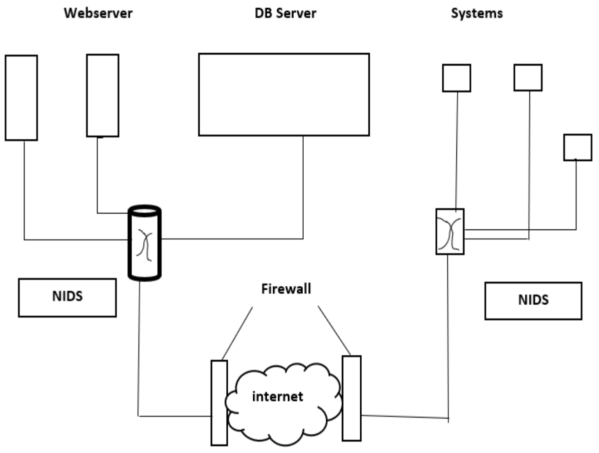


Figure 1: Architecture of NIDS

we understand what are the strategies adopted to detect the intrusion in network packet signature, clustering and machine learning algorithms are used. Clustering is the process of grouping a number of objects so that they are identical to each other in the same category, rather than in other classes. Network clustering finds clusters in a network. Clustering works with two algorithms, which uses label propagation to find appropriate clusters, and other which builds upon the work and adds hop attenuation as a parameter for cluster formation. Network Clustering can help you uncover cliques and highly connected groups in a Network. First, we will use Network to load data set and then we will pass the network through Network Clustering.

In this approach we perform actions based on the analysis in different stages: 1. Input Network. 2. Signature based. 3. Perform Algorithm. 4. Packet filtering. 5. Process data.

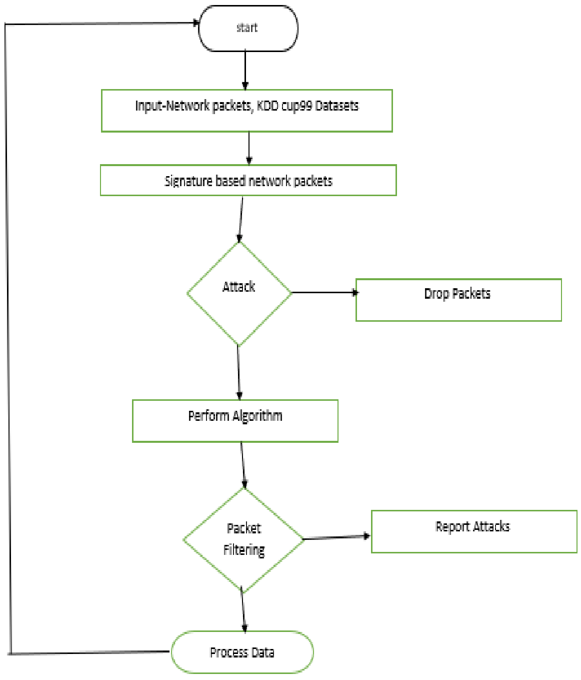


Figure 2: Methodology Flowchart

In this methodology the input network has taken and KDD cup99 dataset used for evaluate or build the IDS. This model will differentiate between bad connections, called attacks or intrusion. When incoming network packets match one the signature of intrusion the system alert the administrator and drop the packets otherwise it will goes to next level in this various algorithms are applied then it will goes to next stage in this every single packet is verified and also report the possible attacks .The last stage of the model is used to process the data it is a continuous process.

III. TRAINING AND TEST SETS

We split the input into 80-20 splits into training and validation sets. After the exercise, both the training set and the test set reach an accuracy of 99 percent. We would assume a lower accuracy in the test set, so we look again at the details and point out that many of the examples in the test set are repeat examples from the training set.

Training data

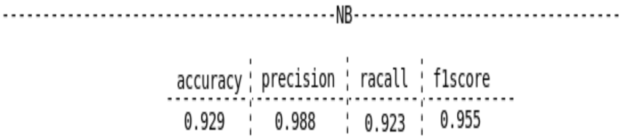
Test data

Fig. 3

IV. RESULTS AND DISCUSSION

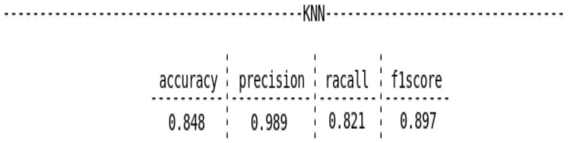
Displaying the Output attributes for the Datasets using Classical Machine Algorithm. The outputs are measured by Accuracy, precision, recall and flscore of input data set.

● Predicting output of Naive Bayes for input test data set.



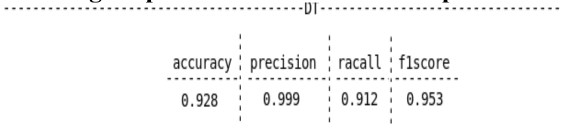
```
------------------------------------NB------------------------------
accuracy ¦ precision ¦ recall ¦ f1score
---------------------------------------------
0.929    ¦ 0.988     ¦ 0.923  ¦ 0.955
```

● Predicting output of K-Nearest neighbors for input test data.



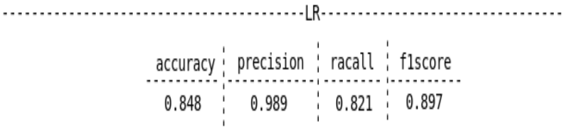
```
-----------------------------------KNN------------------------------
accuracy ¦ precision ¦ racall ¦ f1score
------------------------------------------
0.848    ¦ 0.989     ¦ 0.821  ¦ 0.897
```

● Predicting output of Decision Tree for input test data.



```
-----------------------------------DT------------------------------
accuracy ¦ precision ¦ racall ¦ f1score
------------------------------------------
0.928    ¦ 0.999     ¦ 0.912  ¦ 0.953
```

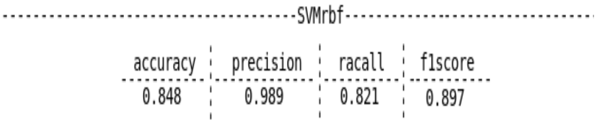
- **Predicting output of Logistic Regression for input test data.**



```
--------------------------------------LR-------------------------------

 accuracy | precision | racall | f1score
 -------------------------------------------
  0.848   |   0.989   | 0.821  | 0.897
```

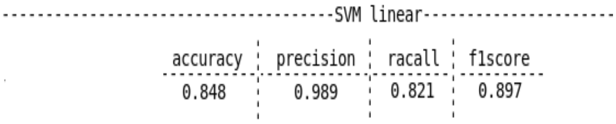
- **Predicting output of SVM Radial Basis Function for input test data.**



```
------------------------------------SVMrbf--------------------------------

 accuracy | precision | racall | f1score
 ------------------------------------------
  0.848   |   0.989   | 0.821  | 0.897
```

- **Predicting output of SVM linear for input test data.**



```
-----------------------------------SVM linear---------------------

 accuracy | precision | racall | f1score
 ------------------------------------------
  0.848   |   0.989   | 0.821  | 0.897
```

Table.1: Accuracy and Precision: Based on the input test data

Input Test Data	Accuracy	Precision
Naïve Bayes	92%	98%
K-Nearest neighbors	84%	98%
Decision Tree	92%	98%
AdaBoost classifier	92%	99%
Random Forest classifier	92%	99%
Logistic Regression	84%	98%
SVM Radial Basis	84%	98%
Svm linear	84%	98%

V. CONCLUSION

In this article, the proposed intrusion detection network architecture provides cluster signatures with the capability to coordinate stronger defense against future network attacks. In addition, the system designed a recent method of pre-processing data in which we extracted unique characteristics from packets that'd been developed and classified as per the implacable potential risk theory of fluidity.

An interesting way forward for future research is to predict which specific network trends direct the device vulnerabilities by examining the data collected in network tables from time to time. It also helps to develop the database of signatures.

REFERENCES

[1] Hoque, Nazrul, et al. "Network attacks: Taxonomy, tools and systems", *Journal of Network and Computer Applications* **40 (2014): 307-324.**

[2] Girardin, Luc. "An Eye on Network Intruder-Administrator Shootouts", In *the Proceedings of the Workshop on Intrusion Detection and Network Monitoring. 1999.*

[3] Lee, Wenke, and Salvatore J. Stolfo. "A framework for constructing features and models for intrusion detection systems", *ACM transactions on Information and system security (TiSSEC)* **3.4 (2000): 227-261.**

[4] R. Lippmann, J. Haines, D. Fried, J. Korba and K. Das. "The 1999 DARPA off-line intrusion detection evaluation". *Computer networks, vol.* ***34****, no.* ***4****, pp.* ***579 595, 2000****. DOI http://dx.doi.org/****10.1016/S13891286(00)00139-0.***

[5] Shankar, Umesh, and Vern Paxson. "Active mapping: Resisting NIDS evasion without altering traffic." *2003 Symposium on Security and Privacy,* **2003**. *IEEE, **2003**.*

[6] Weijian Huang, Yan An and Wei Du, "A Multi-Agent-Based Distributed Intrusion Detection System," ***2010** 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE),* Chengdu**, 2010**, pp. V3-141-V3-143, doi: 10.1109/ICACTE.2010.5579686.

AUTHORS PROFILE

Mrs.Keesara Sravanthi currently working as Assistant Professor, IT Department in VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India. She received her M.Tech in Computer Science and Engineering from JNTUH University, Hyderabad, India. in 2014. Pursuing PhD from GITAM (Deemed to be University),Vizag,India.She is life time member of ISTE and her research interest is Blockchain, IoT, Network Security, Machine Learning, Cyber Security, Artificial Intilligence.

Mr. Gandani Narsing Rao pursed Bachelor of Technology from VNR Vignana Jyothi Institute of Technology, from the Department of Information Technology in 2020. His main research work focuses on Network Security, Cloud Security, Security in Android, Cloud Computing and Privacy, Networking and Computer Intelligence Based Education.

Mr. T Raghu pursed Bachelor of Technology from VNR Vignana Jyothi Institute of Technology, from the Department of Information Technology in 2020. His main research work focuses on Network Security, Cloud Security, Security in Android, Cloud Computing and Privacy, Networking and Computer Intelligence Based Education.

Mr. Pawar Rakesh pursed Bachelor of Technology from VNR Vignana Jyothi Institute of Technology, from the Department of Information Technology in 2020. His main research work focuses on Network Security, Cloud Security, Security in Android, Cloud Computing and Privacy, Networking and Computer Intelligence Based Education.

Mr. A Srinivas pursed Bachelor of Technology from VNR Vignana Jyothi Institute of Technology, from the Department of Information Technology in 2020. His main research work focuses on Network Security, Cloud Security, Security in Android, Cloud Computing and Privacy, Networking and Computer Intelligence Based Education.