IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

Research Paper
Impact Factor - 2.262
Peer Reviewed Journal

HOST BASED DDOS ATTACK DETECTION IN VIRTUALNETWORK SYSTEMS

Gunavathy.K.S* Karthika M.**
**Assistant Professor of B.Com (CA) S.B.K.College, Aruppukottai*
***Assistant Professor of IT,S.B.K College, Aruppukottai*

Abstract
Cloud Computing is a great fortune for IT industries, but the major issue is cloud security. The most common vulnerability is DDoS attack .Distributed Denial of Service is an attack which compromise the entire cloud system and make it to explore. One of the most promising service of cloud computing is Iaas (Infrastructure-as-a- Service) which provides the infrastructure such as load balancer, virtual machine and server required for effective performance and development of an organization. Most of the vulnerabilities occur in Iaas, which is more difficult to detect. To prevent such vulnerabilities, Measurements, and countermeasure selection mechanism called NICE is introduced, which is built on attack graph-based analytical models and Host based Intrusion Detection scheme is used. It improves the overall system efficiency and security.

Keywords: Cloud Computing, Network Security, DDos, NICE.

I. INTRODUCTION

Cloud computing provides resources and services on the internet in a remotely accessible manner. Cloud computing mainly focused on sharing of resources. Cloud computing works based on the concept of virtualization. Cloud computing provides the three basic services such as Iaas, Paas, Saas, ie., it provides the infrastructure which act as the backbone to do any task and provides the platform to process the particular task and also provides the software to execute the task .It minimize the risk and it increases reliability and scalability. It is also less expensive and it provides lot of benefits to the organization. There is no need for an organization to buy a server and other infrastructures required to store and process the data. It enhances the efficiency and performance of the system. Cloud computing enables multiple users to share and access resources.

Today most of the organization uses cloud computing technology because of its low cost, high speed, availability and itís on demand service nature. The data which we stored in cloud can be maintained easily and location independent. In cloud computing technology clouds are categorized in to public, private and hybrid clouds. There is a lack of security in cloud computing, it should be improve.

II.RELATED WORK

A. *Attack Graph Model:* An attack graph is a demonstrating tool to illustrate all promising attack paths which are essential to understand threats and then to decide appropriate countermeasures and action. In that attack graph, each node represents the consequence of the vulnerabilities. It protects the system from vulnerabilities and improves system performance.

B. *Alert correlation graph:* Alert Correlation graph provide alert while it detect vulnerabilities, it helps to prevent the system from attacks. But there may be a chance of false alarm. It makes the system inefficient. To overcome that Host based intrusion detection technique is introduced, which reduces false alarm rate.

C. *Counter Measure Selection: This* algorithm shows how to select the optimized countermeasure based on vulnerabilities. The alert is provided only after the attacker attacks the system. It helps to reach the target with minimum distance and prevent the system from vulnerabilities. It reduces time consumption and makes the system more efficient.

III.PROPOSED METHODOLOGY

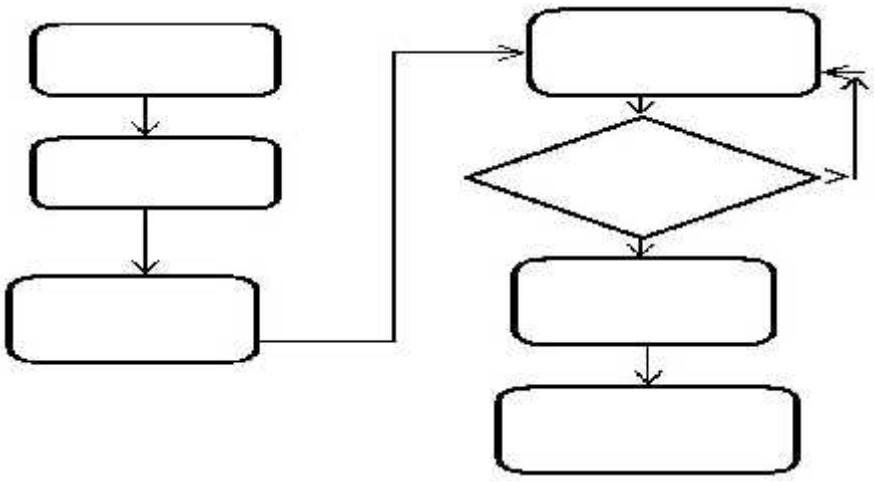
The proposed methodology introduces Host based intrusion detection to improve the detection accuracy and to avoid loopholes in the cloud .Host based intrusion detection technique detects all kind of vulnerable attacks including DDos attack. It works on the concept of virtualization .By thisconcept the attack of the DDos effect can be reduce. If there is a problem in one virtual machine of virtual network it will not be reflect in other virtual machines. If any vulnerable user enters into the system, the alarm will inform it to the network controller .This intrusion technique reduces the rate of false alarm. It increases the overall system efficiency. The basic detection and countermeasure algorithm is used and the alert correlation algorithm is used to detect the attacks. The attack graph model generates the graph automatically where

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

the attacks will happen frequently.

The contributions of NICE are presented as follows:
We devise Host Based intrusion detection and countermeasure selection and vulnerabilities that handle and inspect uncertain cloud traffic without interrupting usersí applications and cloud services.
The framework consists of 1.NICE-Agent on each physical cloud server, 2. Network controller, 3. VM profiling server, 4. Attack analyzer

a. *NICE-A:* It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers.
b. *VM profiling***:** VM profiles are maintained in a database and contain comprehensive information about vulnerabilities, alert, and traffic. The dataís are comes from attack graph generator, network controller, NICE-A.
c. *Attack analyzer:* The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation, and countermeasure selection.
d. *Network controller:* The network controller is responsible for collecting network information of current Open Flownetwork and provides input to the attack analyzer to construct
attack graphs.



IV RESULTS FOR PROPOSED METHODOLOGY

A. Simulation Result for Security metrics Measurement

In Fig.2, the NICE system scans the virtual network and check any vulnerabilities are present, if it so it triggers countermeasure selection algorithm to take necessary action .It receives packet and find out the vulnerable packets and classify it based on vulnerabilities.

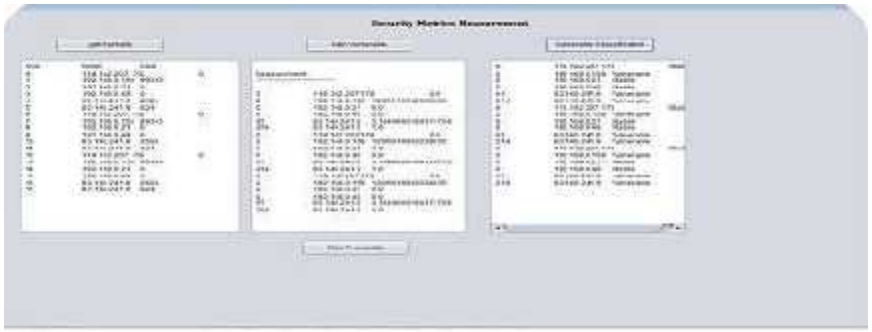


Fig.2. Simulation Result for security metrics measurement

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

B. Simulation Result for Countermeasure action

InFig.3, it shows which source IP is vulnerable and which causes suspicious effect to the system.

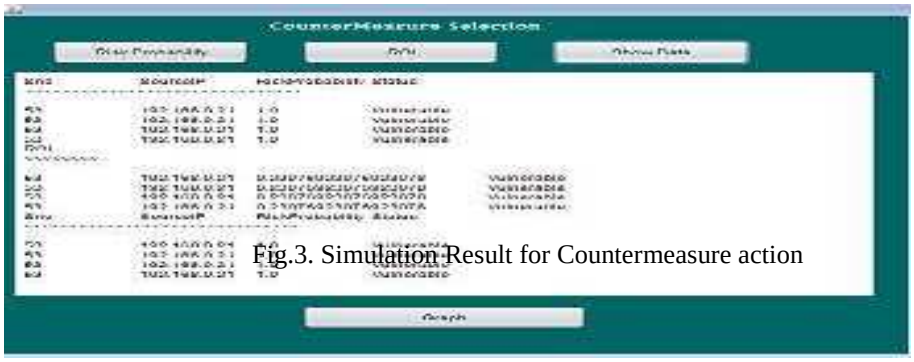


Fig.3. Simulation Result for Countermeasure action

V.PERFORMANCE EVALUATION

A. Results and Discussions

To determine the viability of our solution, reasonable studies were conducted on several virtualization approaches. Evaluated NICE based on Dom0 and DomU implementations with mirroring-based and proxy based attack detection agents (i.e., NICE-A). In every virtual machine NICE-A is deployed which is connected to the monitor network to handle the traffics in the network using Switched Port Analyzer (SPAN) approach. When the IDS is running in Intrusion Prevention System (IPS) mode, it needs to intercept all the traffic and perform packet checking, which requires more system resources when compared to IDS mode.

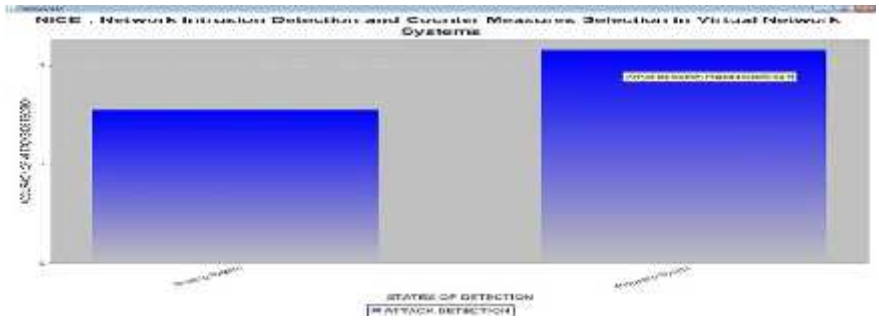


Fig. 4. Performance analysis graph

VI. CONCLUSION AND FUTURE WORK

NICE, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches-based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of NICE and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers. A dynamic multiphase detection system with higher detection accuracy is proposed to detect and mitigate the various attacks. The detection covers the whole spectrum of the intrusion detection system. The HIDS is incorporated in the existing NICE concept to improve the detection accuracy of the system. The cloud is configured into two networks virtually. This will reduce the risk of spreading of the zombie to the rest of the network.

Further research will investigate the improvement of the overhead of the intrusion detection system. Additionally, investigate the scalability of the proposed NICE solution by investigating the decentralized network control and attack analysis model based on current study. The false alarm rate has to be improved to get a higher efficient detection system and countermeasure attacks.

REFERENCES

1. Chun-Jen Chung; Khatkar, P.; Tianyi Xing; Jeongkeun Lee; Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," *IEEE Trans.Dependable and Secure Computing* , vol.10, no.4, pp.198,211, July-Aug. 2013.
2. Huaibin Wang Haiyun Zhou and Chundong Wang china.,î *Virtual Machine based Intrusion Detection System Framework in Cloud Computing Environment*î, journals of computer and communication VOL.7, NO.10, pp. 23,97 OCTOBER 2012.
3. N. Poolsappasit, R. Dewri, and I. Ray, ì*Dynamic Security Risk Management Using Bayesian Attack Graphs,*î IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb,2012.
4. B.Joshi,A.Vijayan,and B.Joshi, ìSecuring Cloud Computing Environment Against DDoS Attacks,îProc.IEEE Intíl Conf.Computer Comm. And Informatics (ICCCIí12), Jan.2012.
5. Z.Duan, P.Chen, F.Sanchez, Y.Dong, M.Stephenson, J.Barker,ìDetecting Spam Zombies by Monitoring Outgoing Messages,îIEEETrans.DependableandSecureComputing, vol.9, no.2, pp.198-210, Apr.2012.
6. B. Joshi, A. Vijayan, and B. Joshi, ì*Securing Cloud Computing Environment Against DDoS Attacks,*î Proc. IEEE Intíl Conf. Computer Comm. and Informatics (ICCCI í12), Jan. 2012.
7. G.Gu, J.Zhang, andW.Lee, ìBotSniffer: Detecting Botnet Command and Control Channels in Network distributed Sytem Security Symp. (NDSSí08).
8. O.Sheyner,J.Haines,S.Jha,R.Lippmann,J.M.Wing, automated Generation and Analysis of Attack raphs,îProc.IEEESymp. Security and Privacy,pp.273-284,2002.