International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Zombie Avoidance using Attack Analyzer in Cloud Environment

[1]K. Periasamy
Research Scholar
Information and Communication Engineering
Anna University,
Chennai, India

[2]B. Latha
Professor and Head
Computer Science and Engineering
Sri Sairam Engineering College
Chennai, India

***Abstract*-- Cloud Computing refers to On-demand network access to a shared pool of manageable computing resources which are applicable to both software and hardware services. Cloud Computing makes use of available resources on "on-need" basis. Security problem plays the most Significant role in cloud computing. Due to this nature, attackers launch Distributed Denial of Service to make resources unavailable to potential users. Usually, Denial of Service easily attacks the virtual machines as Zombies but it is extremely hard to detect Zombies. In this paper, we have proposed a viable approach to prevent the vulnerable virtual machine from Zombies through multi-phase distributed susceptibility detection, measurement and countermeasure selection mechanism called NICE. This experimental model shows a more secure and reliable network access to reconfigure the virtual network.**

***Index Terms*-** *Cloud Computing, Attack Graph, Zombie Detection, Network security*

I. INTRODUCTION

The current adoption of Cloud Computing enables us to utilize the available resources on the basis of On-demand network access and computing resources such as networks, storage, service, application and servers. The five vital characteristics of cloud computing includes on-demand service, rapid elasticity, location-independence, ubiquitous network access and measured service, which are geared toward using clouds flawlessly and visibly. DDoS is one of the major threats that break the business continuity service availability, accessing the resources and making more traffic as legitimate as web traffic in order to launch various attacks.

II. VIRTUAL MACHINE AS ZOMBIES

Compromised machines are one of the major challenges in cloud system which are used to launch various security threats to make the resources unavailable. Such compromised virtual system grouped together are called virtual machine as Zombies. Within the cloud system, particularly the Infrastructure-as-a-Service (IaaS) clouds, the detection of such zombie exploration attacks is tremendously difficult because cloud users may install vulnerable applications on their virtual machines. To prevent such susceptible virtual cloud system from being compromised, we proposed NICE mechanism to provide countermeasure against Zombies with help of an attack graph-based model.

III. INFRASTRUCTURE AS-A-SERVICE

Infrastructure-as-a-Service (IaaS) is a service delivery model that provides the basic computing utility infrastructure such as servers, software and network equipment on the basis of on-demand services. The major purpose is to avoid the basic hardware components and software components purchasing, housing, and managing those infrastructure components, instead achieve those resources as virtualized objects from service interface. The cloud consumer usually has wide options to choose the operating system and development environment to be hosted. Thus, the detection of zombies at Infrastructure as-a service makes it difficult because users may install vulnerable application software on their virtual machine system and the combined effect of vulnerability is not measured.

IV. ATTACK ANALYZER

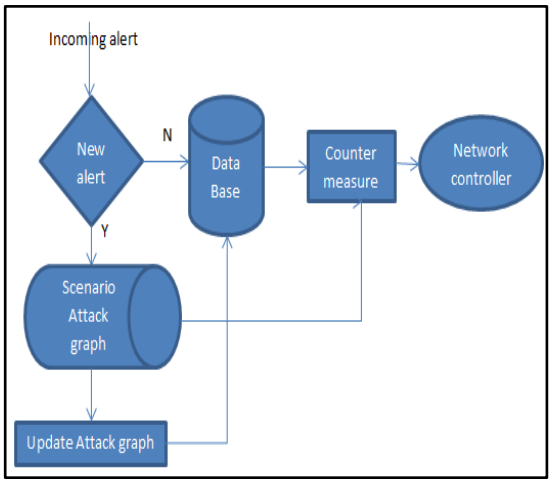


Fig. 1 Monitoring and Updating Attack Graph

NICE-Agent scans the whole cloud network periodically, once it discovers vulnerability in cloud network it generates an alert and sends it to attack analyzer. Each path is a successful attack. Attack analyzer checks whether the alert is new or not. If the incoming alert is of

new vulnerability and is not present in the attack graph, the attack analyzer inserts the alert into the attack graph and then reconstructs it. Once construction gets completed, attack analyzer provides the countermeasure that is applied by the network controller based on the severity of evaluation results. Thus, we implement NICE mechanism to provide countermeasure against attacks.

V. IMPLEMENTATION

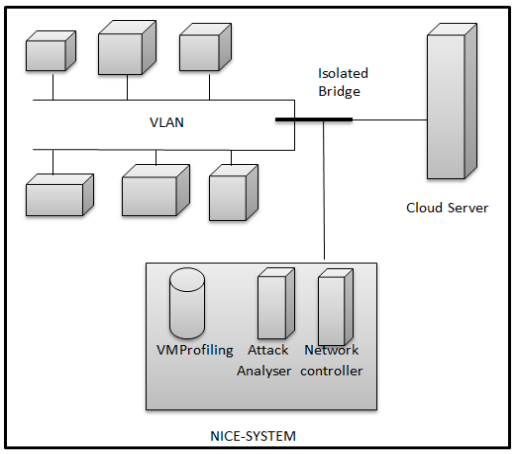


Fig. 2 Architecture of NICE System

NICE- A is implemented in isolated bridges that are located between VM and Cloud server. NICE analyzes the cloud traffic with the help of a light weighted mirroring based detection agent. Traffic generated by attacker through the virtual machine is monitored by NICE-A. Based on vulnerability, it generates and alerts the attack analyser. Attack analyser checks if it is new or not, if alert is old, selects appropriate countermeasure otherwise construct SAG with the information gained from network controller, VM profiling and conducting some penetration test, VM profiling is a database that contains information about state, service running in VM, traffic vulnerability which is from SAG and NICE-A and it select countermeasure which is send it to the network controller, which isused to implement countermeasure and updates SAG.The countermeasure is based on dynamic that reconstruct filtering rules, rearranging allow & deny conditions, achieved by software switch which is controlled by network controller. So we are providing dynamic production against attack. NICE sniffs the traffic generated by attacker using SPAN. So the new affects original traffic. NICE allows the cloud server to provide service to requested client continuously, at the same time it provides security to cloud server.

VI. PERFORMANCE METRICS

Security matrices are needed to assess the risk. The distance to every target node must be determined before countermeasure selection. If the distance is too long, a countermeasure should not be selected, instead we update the ACG for an alert.

A. CPU utilization

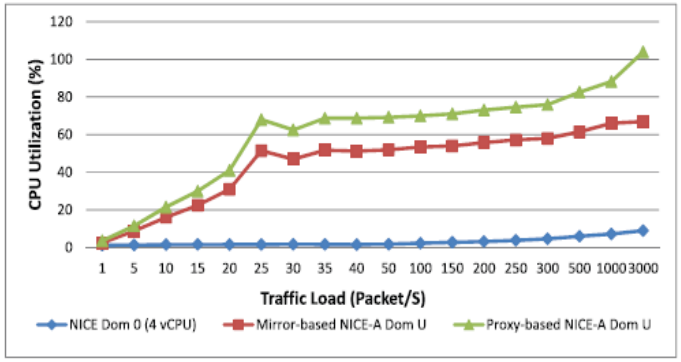


Fig.3 CPU utilization graph

NICE-A Dom O is better way for IDS because it utilizes less amount of CPU process that can be installed at bridges level

B. Network communication delay

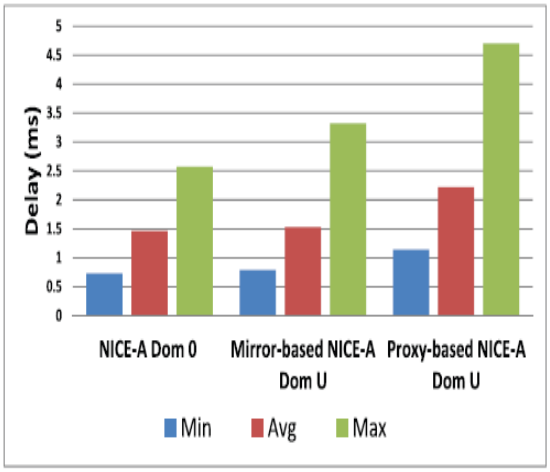
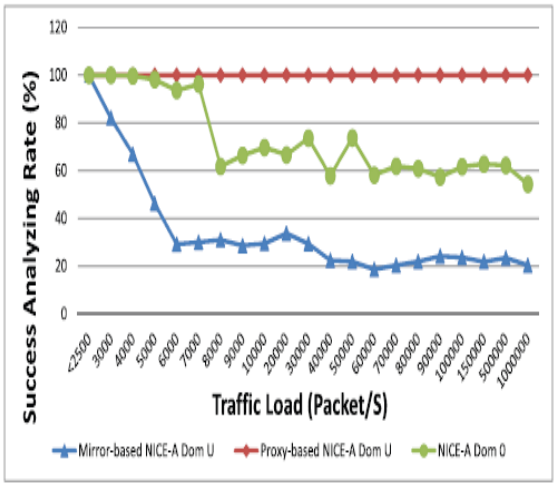


Fig. 4 Performance of Network Communication

NICE–A Dom O is better because it uses SPAN to monitor traffic which makes less amount of delay. NICE-A Proxy based use original traffic to monitor the incoming outgoing packet

C. *Success Measure Rate*



Success analyze rate= No of analyzed packet/Total received packet

NICE-A Dom U is better because it uses original net traffic and it never bothers about packet delay.

With the attack graph, we can get a holistic view of the security condition and make predictions.

VII. CONCLUSION

In this paper, we presented NICE to protect cloud virtual networking environment from DDoS attack. NICE construct attack graph predicts the next step of the attackers and provides optimized countermeasure. NICE software switches implement the countermeasure against zombie explorative attack dynamically. To improve the detection accuracy, NICE are needed to be implement in distributed fashion. The proposed solution can reduce the risk of cloud system being misused by internal and external attack. The experimental results show less amount of CPU utilization and better success measure rate of traffic load.

REFERENCES

[1] Chun-Jen Chung, Tianyi Xing, Pankaj Khatkar, Jeongkeun Lee,Dijiang Huang, on "*NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems*" IEEE transaction on dependable and secure computing, no.4,vol. 10, , pp. 198-211, 2013 July/Aug..

[2] Lizhe W. and Gregor V. L. ,(2008), " a Perspective Study: Cloud Computing," volume 28 of Computing's new Generation, Number 2, 137-146, DOI: 10. 1007/s00354-008-0081-5

[3] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi "*Securing Cloud Computing Environment Against DDoS Attacks"2012 internatio*nal conference on computer informatics and communication Jan. 2012.

[4] Hassan Takabi and James B. D. Joshi *University of Pittsburgh* Gail-Joon Ahn *Arizona State University* www. computer. org/security COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES 1540 7993/10/$26. 00 © 2010 IEEE NOVEMBER/DECEMBER 2010

[5] Bouzida Y, Cuppens F, Gombault S, (2006) on "Detecting and Reacting against Distributed Denial of Service Attacks,"IEEE International Conference on Communication. Volume 5

[6] Wayne Jansen, Timothy Grance, (Dec. 2011), "Guidelines on Security and Privacy in Public Cloud Computing" NLST-National Institute of standards and Technology, US Department of commerce , a special publication 800-144

Authors Biography

K. Periasamy received the M. E Degree in Computer Science and Engineering from KSR College of Technology, Namakkal, India in 2005. He is currently doing his doctorate degree in Anna University, Chennai and working as an Associate Professor at Sri Sairam Engineering College, Chennai, India and his area of interest are wireless networks and cloud computing.

Dr. B. Latha graduated from Annamalai University (BE/CSE), India in 1998 and received her Master's in Computer Science and Engineering from Sathyabama University, India in 2005 and completed her Doctorate Degree in the Faculty of Information and Communication Engineering, Anna University Chennai, India in 2010.Currently she is working as the Head of the Department and a professor, in the Department of CSE in Sri Sairam Engineering College, Chennai, India. She has published her paper over 13 International Journals and presented papers in 9 International conferences and 9 National conferences and also she has published 2 books. She is a member of IEEE, CSI,IACSIT and life member of ISTE. Her current research interest include Artificial Intelligence, Network Security, Machining of composite materials, Computer aided modeling and optimization. She is guiding 11 Ph. D research scholars.