IJCAT - International Journal of Computing and Technology, Volume 1, Issue 9, October 2014
ISSN : 2348 - 6090
www.IJCAT.org

NICE: Network Intrusion Detection, Prevention and Countermeasure Selection in Virtual Network Systems

[1] Mandar Mahadeokar, [2] Suresh Rathod

[1, 2] Department of Computer Engineering, Sinhagad Academy of Engineering, Kondhwa (University of Pune), Pune, Maharashtra, India

Abstract - Cloud security is one of most important issues that need a lot of research and development effort in past few years. Particularly, attackers can find out the vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multi-step xploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks can be takes place through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which provides reconfigurable virtual network-based countermeasures. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

Keywords **- Network Security, Cloud Computing, Intrusion Detection, Zombie Detection.**

1. Introduction

Cloud computing is internet-based computing in which allow large groups of remote servers to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources. Cloud computing is not a programming language it is just a way to use old services very effectively. In computer security, a Network Intrusion Detection System (NIDS) is intrusion detection systems that try to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. A recent CSA (Cloud Survey Alliance) survey reports that among all Security issues exploitation and despicable use of cloud computing is considered as the main security threat. In traditional data centers, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security holes in cloud data centers, where cloud users usually have the privilege to control software installed on their managed VMs, may not work effectively and can violate the Service Level Agreement (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users.

In a cloud system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs.

In this article, we propose NICE (Network Intrusion detection and Countermeasures Election in virtual network systems) to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack detection procedures into the intrusion prevention processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE only provides software framework which is useful for attack detection, appropriate counter measure election and finally NICE also provides Security policies which will help in securing the overall cloud environment.

2. Existing System

Cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. In a cloud system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs

2.1 Disadvantages of Existing System

1. No detection and prevention framework in a virtual networking environment.
2. Not accuracy in the attack detection from attackers

3. Proposed System

3.1 NICE System

To In this article, we propose NICE (Network Intrusion detection and Countermeasures Election in virtual network systems) to establish a defense-in-depth intrusion detection framework.

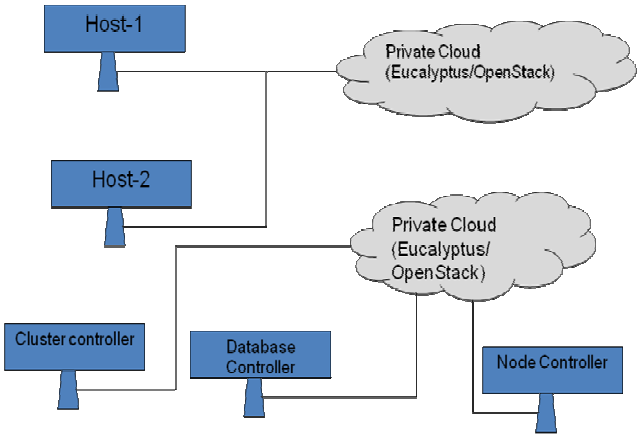

Fig. 1 Proposed Nice Model

For better attack detection, NICE incorporates attack detection procedures into the intrusion prevention processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE only provides software framework which is useful for attack detection, appropriate counter measure selection and finally NICE also provides Security policies which will help in securing the overall cloud environment.

4. Conclusions

NICE, proposed to detect and identify collaborative attacks in the cloud virtual environment. NICE conduct attack detection and prediction. It only investigates network IDS approach to detect/find out zombie explorative attacks. In order to improve the detection accuracy, host-based IDS solutions are needed to be consider which cover the whole spectrum of IDS in the cloud system. And also existing system does not provide any mechanism for attack prevention, so this drawback is overcome in proposed system.

References

[1] O.Database, "Open source vulnerability database (OVSDB)," http://osvdb.org/. 2012.

[2] Chun-Jen Chung, Student Member, IEEE, Pankaj Khatkar, Student Member, IEEE, Tianyi Xing, Jeongkeun Lee, Member, IEEE, and Dijiang Huang Senior Member, IEEE "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE, Vol. 10, No. 4, Year 2013.

[3] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter:detecting malware infection through IDS-driven dialog correlation," Proc. of 16th USENIX Security Symp. (SS '07), pp.12:1–12:16, Aug. 2007.

Mandar M. Mahadeokar received the B.E. degree in Computer Engineering from A.I.S.S.M.S.COE,Pune, INDIA in 2013 and perusing M.E. degree in Computer Engineering from S.A.O.E , Pune

Suresh B.Rathod received the B.E. degree in Computer Engineering from T.COE,Tulajapur INDIA in 2007 and M.E. degree in Computer Engineering from S.C.O.E, Pune in 2012.He is currently working asa Assistant Professor in S.A.O.E,Pune.