Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5494

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

Miss. Rakhi. R. Patel
Third year Computer Science & Engineering Student,
Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal
North Maharashtra University Jalgaon, Maharashtra - 425203, India
rakhipatel18@gmail.com

ABSTRACT:
Today cloud computing has increased in many organization, and then the cloud security is very important issue. This is because cloud user can install can install vulnerable software on their virtual machine. To prevent vulnerable virtual machine from being compromised in the cloud, the network intrusion detection and countermeasure selection mechanism is proposed called as NICE. It detects and minimizes attacks in cloud server and it significantly reduces the risk of cloud system from abused by internal and external attackers.

Keywords: cloud Security, Cloud Computing, Intrusion Detection, Attack Graph, DDOS.

I. INTRODUCTION

Recent studies have shown that users migrating to the cloud consider security as the most important factor. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. A recent Cloud Security Alliance (CSA) survey shows that among all security issues, nefarious and abuse use of cloud computing is considered as the top security threat, in which attackers can take advantage of vulnerabilities in clouds and utilize cloud system resources to deploy attacks. The vital attack to be prevented is Distributed Denial of Service (DDOS) attacks in cloud computing environment. These attacks usually involve early stage actions such as low-frequency vulnerability scanning, multistep exploitation, and compromising identified vulnerable virtual machines and finally DDOS attacks through the compromised zombies [2]. Within the cloud system, the detection of zombie exploration attacks is extremely difficult, especially in the Infrastructure-as-a-Service (IaaS) clouds, because cloud users may install vulnerable applications on their virtual machines. To prevent this condition a network intrusion detection and Counter Measure Selection Mechanism called NICE is proposed, it is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures [1].

II. EXISTING SYSTEM

In the existing system there is a data center, where system administrators have full control over the host machines, vulnerabilities can be detected by the system administrator in a centralized manner. Patching known security holes in cloud data centers, where cloud users usually have the right to control software installed on their managed VMs. It may not work essentially and can break the Service Level Agreement (SLA) [1, 2]. Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to exception in cloud security. The challenge is to establish an efficient vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users [4].

A. Disadvantages

- When an attacker attacks to the user or server in network which are especially infrastructure as a service based server then detection of effected server are externally difficult because of cloud user may install multiple types of software in the server with their user account.
- This model can generate all possible attack paths; then the big issue for this solution is scalability.
- System performance is low because users of cloud may install unprotected application on their virtual machines.
- It provides the low security.

III. PROPOSED SYSTEM

In the Proposed System, Network Intrusion detection and Countermeasure Selection is establish a defense-in-depth intrusion detection framework for better attack detection, Network Intrusion detection and Countermeasure Selection incorporates attack graph analytical procedures into the intrusion detection processes. When an attacker attacks to the

server by using a user account, attacker can deploy multiple levels of malwares to the server, if and only if he can access to the server, but in existing system it's hard to detect the attacker because of server cloud service. While in proposed, when an attacker attacks the server using user account, the attack analyzer can detect the attacker and send the warning to administrator that user (attacked by the zombie) try to access to other users account to deploy the multiple levels of malware and admin waits for maximum attempts and then admin blocks him permanently using scenario attack graph. The design of NICE uses a reconfigurable virtual networking approach to detect and count the attempts to compromise VMs, so preventing zombie VMs.

IV. SYSTEM ARCHITECTURE

The proposed system is designed to work in a cloud virtual networking environment. It consists of a cluster of cloud servers and their interconnections. The deployed security mechanism focuses on providing a non-intrusive approach to prevent attackers from exploring vulnerable VMs and use them as a stepping stone for further attacks. Major components in NICE framework are distributed and light-weighted network intrusion detection agent (NICE-A) on each cloud server, a VM profiling server, a attack analyzer, and a network controller [3, 4].

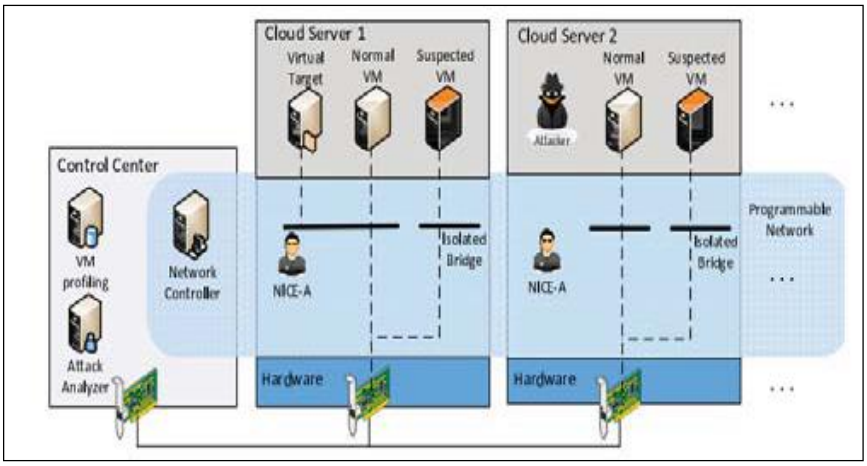

Figure 1:- NICE Architecture [8]

A. Module description

- **NICE-A**

  Network intrusion detection agent (NICE-A) is deployed on each cloud server to capture and analyze cloud traffic. It scans the virtual system vulnerabilities within a cloud server. When suspicious or unprotected traffic is detected intrusion detection alerts are sent by NICE agent to Attack analyzer [1].

- **VM Profiling**

  Virtual machines in the cloud can be profiled to get information about their services running, state, open ports, etc. it also contains details about its connectivity with other VMs. Knowledge of services running on a VM is required to verify the authenticity of alerts belongs to that VM. An attacker can examine the network to look for open ports on any VM by using port scanning program. Information about open ports on a VM and the history of opened ports plays a significant role in determining how vulnerable the VM is. And VM profile form by combining all these factors. VM profiles are maintained in a database and contain information about alert, traffic and vulnerabilities [1].

- **Attack Analyzer**

  The major functions of attack analyzer includes attack graph construction, update, alert correlation and countermeasure selection [5,6].The process of constructing and utilizing the Scenario Attack Graph (SAG) consists of three phases such as information gathering, potential exploit path analysis and attack graph construction [5]. With this information, attack paths can be modeled using SAG. When attack analyzer receive the alert from NICE-A, it matches the alert in the ACG. If received alert already exists in the graph, the attack analyzer performs countermeasure selection procedure and then notifies network controller to deploy the countermeasure actions [1].

- **Network Controller**

  Network controller is responsible for collecting network information and provides input to the attack analyzer to construct attack graphs [5]. Network controller is also responsible for applying the countermeasure [6]. Based on optimal return of investment and risk probability of the node countermeasures are selected by attack analyzer and executed by network controller [1].

B. Algorithm used

- **Alert Correlation**

  Alert correlation can predict the possible threats and attacks by correlating detected events or activities. If the event is recognized as potential attack, it can apply specific countermeasures to reduce its impact or take action to prevent it from damaging the cloud system [5].

- **Countermeasure Selection**

  Countermeasure used to reconfigure the virtual network-based system and monitor, control plane over distributed programmable virtual switches to significantly improve attack detection. Countermeasure is an process, action, system or device that can prevent or reduce the effect of threats to a computer server or network. Countermeasure are selected by attack analyzer and executed by network controller [6].

C. System configuration

1. **Hardware Configuration**

- Processor - Pentium –IV
- Speed - 1.1 GHz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor – SVGA [7]

2. **Software Configuration**

- Operating System: Windows XP
- Programming Lang.: JAVA/J2EE
- Java Version: JDK 1.6 & above [1, 7].

V. ADVANTAGES

- NICE significantly advances the current network IDS/IPS solutions by using programmable virtual networking approach that allows the system to construct a dynamic reconfigurable IDS system.
- NICE, a new multi-phase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious cloud traffic without interrupting users' applications and cloud services [7].
- NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Because of programmable network approaches, NICE can improve the probability attack detection and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services [7].
- NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behaviour and also suggests effective countermeasures [7].
- NICE optimizes the implementation on cloud servers to minimize resource consumption. NICE study shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions [7].

VI. CONCLUSION

NICE, which is proposed to detect and reduces collaborative attacks in the cloud virtual networking environment. And it uses the attack graph model to conduct attack detection and prediction. The proposed solutions examine how to use the programmability of software switches based solutions to improve the detection accuracy. System performance evaluation shows the feasibility of NICE and also shows that the proposed solution can significantly reduce the risk of the cloud system from being utilize and abused by internal and external attackers.

NICE only investigates the network IDS approach to counter zombie explorative attacks. In future to improve the detection accuracy, host-based IDS solutions are required to be incorporated and to cover the whole spectrum of IDS in the cloud system. This should be examining in the future work. Furthermore, the scalability of the proposed NICE solution will investigate by researching the decentralized network control and attack analysis model based on current study.

ACKNOWLEDGMENT

I feel great pleasure in submitting this Paper on "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network System"**.** I wish to express true sense of gratitude towards my H.O.D., Prof. D. D. Patil. I also wish to thank my teacher Mr. Y. S. Patil who at very discrete step in preparation of this Paper contributed his valuable guidance and help to solve every problem that arose. Also, most likely I would like to express my sincere gratitude towards my family for always being there when I needed them the most. With all respect and gratitude, I owe my all success to the writers of reference papers that are referred by me in completion of this paper work activity which will be useful in presenting my survey paper.

REFERENCES

[1] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, "Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE Trans. Dependable and Secure Computing, vol. 10, no. 4, July/August 2013.

[2] B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," in Computer Communication and Informatics (ICCCI), 2012 International Conference on, Jan. 2012, pp. 1 –5.

[3] H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, Dec. 2010.
[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," ACM Commun., vol. 53, no. 4, pp. 50–58, Apr. 2010.
[5] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," Computational Intelligence in Security for Information Systems, LNCS, vol. 6694, pp. 58–67.Springer, 2011.
[6] Roy, D. S. Kim, and K. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," Proc. IEEE Int'l Conf. on Dependable Systems Networks (DSN '12), Jun. 2012.
[7] International Journal of Computer Science Engineering and Technology (IJCSET) | May 2014 | Vol 4, Issue 5.
[8] Journal of international academic research for multidisciplinary, Volume 2, Issue 4, May 2014.