IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 84-88
www.iosrjournals.org

Detection of Network Intrusion and Countermeasure Selection in Cloud Systems

Mr .Madhusudan S, Mr .Srikanth S.P
Department .of CSE MVJ College of Engineering Bangalore, India
Associate Professor,Dept of CSE MVJ College of Engineering Bangalore, India

***Abstract*:** *In Cloud Server Systems, The detection of zombie in virtual machine is considered as the security threat exploration attacks is extremely difficult, due to this the cloud user can able to install harmful applications into their virtual server to attack the virtual server Particularly, intruders can exploit vulnerability to a cloud system and compromise virtual machines to deploy further large scale types of attack like distributed denial of service (DDOS). Mainly vulnerability arises in infrastructure as a service (laas) cloud where the infrastructure shared by millions of users. To prevent vulnerable virtual machine from being compromised in the cloud, the proposed framework introducing multiple distributed vulnerability detection network intrusion and countermeasure selection in cloud systems. It built an attack graph analytical model which is used for identify the intruders possible way of exploit vulnerability.*
Index Terms: *Cloud Computing ,SLAs,DDOS ,IaaS, Virtual machine, Vulnerability, Command And Control.*

I. INTRODUCTION

In Recent studies have shown that users migrating to the cloud consider security as the most important factor. A recent Cloud Security Alliance (CSA) survey shows using of cloud computing is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to attack it. In data centers, the system administrators have full control over the host system, defect can be detected and rectified by the system administrator. However, rectifying known security holes in cloud server, where cloud users usually have the rights to control software installed on their managed VMs, may not work properly and can affects the *Service Level Agreement* (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which leads to loopholes in security. The difficult 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, M. Armbrust *et al[2]*. addressed that protecting"Business continuity and services availability" from service outages is one of the top concerns in Cloud Computing systems. In a cloud system where the infra structure is shared by potentially many users attacked by 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., sharing the same data and file systems, even with attackers. The same setup for VMs in the cloud, e.g., virtualization method, VM OS, installed harmful software, networking, etc., attracts attackers to attack multiple VMs. In this article, we propose NICE (Network Intrusion detection and Counter measures Election in virtual network systems)[1] to establish a defense-in-depth intrusion detection. attack detection, NICE uses attack graph analytical procedures into the intrusion detection processes. NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to attack VMs, that preventing zombie VMs. In general, NICE includes two main phases:

- Deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A repeatedly scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability.
- Once a VM enters inspection state, (DPI) Deep Packet Inspection is applied, virtual network reconfigure tions can be deployed to the inspecting VM to make the potential attack behaviors.

II. Related Works

Z.Duan, P.Chen, F.Sanchez[5] "Detecting spam zombies by monitoring Outgoing messages", Compromised machines are one of the key security threats on the internet, they are often used to launch various security attacks such as spamming and spreading malware, DDOS, and identify theft. Given that spamming provides a key economic incentive for attacks to recruit the large number of compromised machines.develop an effective spam zombie detection system named SPOT by monitoring outgoing messages of a network. G.Gu, J. Zhang "BotSniffer: Detecting Bonet command and Control channels in Network traffic", Bonets[7] are recognized as one of the most serious security threats. In contrast to previous malware, botnets have the characteristics of a command and control channel. This makes the detection of bonet a challenging problem. It proposing an approach that uses network-based anomaly detection to identify botnet channels. O.Sheyner[8], J.Haines "An integral part of modeling the global view of network security is constructing attack graphs". Using automated technique for generating and analyzing attack graphs.

The technique on symbolic model checking algorithms, letting us constructs attack graphs automatically and efficiently. B.Joshi[4], A.vijayan[3] "Securing cloud computing environment against DDOS attacks", Focusing on detecting and analyzing the distributed denial of service (DDOS)attacks in cloud computing environments. This type of attacks is often the source of cloud service disruptions. The solution is to combine the evidences obtained from intrusion detection systems (IDSs). G.Gu, P.Porras, V.Yegneswaran, M.Fong, and W.Lee[6] "BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation", the malicious software The malicious software or malware has risen to become a primary source of most of the scanning (distributed) denial-of-service (DOS) activities and direct attacks, taking place across the Internet. Among the various forms of malicious software, botnets in particular have recently distinguished themselves to be among the premier threats to computing assets. Like the previous generations of computer viruses and worms, a bot is a self-propagating application that infects vulnerable hosts through direct exploitation or Trojan insertion. All bots distinguish themselves from the other malware forms by their ability to establish a command and control (C&C) channel through which they can be updated and directed. Once collectively under the control of a C&C server, bots form what is referred to as a botnet. L.Wang[13], A.Liu and S.jajodia, "Using Attack graphs for Correlating, Hypothesizing and Predicting Instrusion Alerts," A network intrusion that is composed of multiple attacks preparing for each other can infiltrate a wellguarded network. Defending against such multi-step intrusions is important but challenging. It is usually impossible to respond to such intrusions based on isolated alerts corresponding to individual attack steps. The reason lies in the well-known impreciseness of Intrusion Detection Systems (IDSs). That is, alerts reported by IDSs are usually filled with false alerts that correspond to either normal traffic or failed attack attempts. To more effectively defend against multi-step intrusions, isolated alerts need to be correlated into attack scenarios.

III. 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 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.

*Disadvantage of exiting system***:**

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

IV. System Architecture

The architecture of NICE[1] system explains complete prevention of zombie exploration by the intruders by taking countermeasures by intruders.

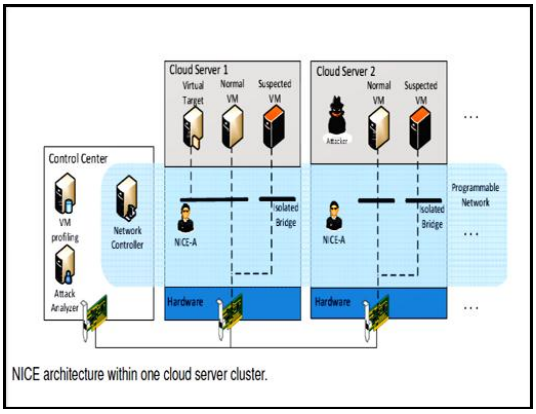

Figure 1: System Model

The NICE framework within one cloud server cluster. Major components in this framework are distributed light-weighted NICE-A on each physical cloud server, a network controller a VM profiling server, and an attack analyzer.The latter three components are located in a centralized control center connected to software switches on each cloud server. NICE-A is a software agent implemented in each cloud server connected to the control center through a dedicated and isolated secure channel, which is separated from the normal data packets using open flow tunneling or VLAN approaches. The network controller is responsible for deploy attack countermeasures based on decision made by the attack analyzer.

V. Proposed System

In Proposed system, avoiding a compromising virtual machine in cloud environment introducing a multiphase distributed vulnerability detection measurement in multiple server clusters. In that NICE-A[1] periodically scans the server if any vulnerability is present means it raised one alert that alert send to the control center there attack graph starts to construct the attack graph to identify the attack which is raised by intruders. After detected a particular attack in the Control center made appropriate counter measure by the network controller. It arises several advantages that are better security, reducing the risk of cloud system; vulnerable virtual machines avoided, and improved accuracy.

a) Modules

- Cloud service provider
- Cloud User
- NICE-A
- Attack Analyzer
- Network Controller
- VM Profiling
- Performance Evaluation

b) Modules description

- **Cloud Service Provider:**

A Service Provider offers customer's storage or software service available via a private or public network from a cloud computing provider's servers as opposed to being provided from a company's own onpremises servers.

- **Cloud User:**

The provider allows an authenticated userto allow accessing a cloud space. For storing or retrieving a file or any applications. The cloud user able to storing a file or a file or a data in encrypted and the data can be retrieved by decryption.

- **NICE-A:**

The NICE-A is a network intrusion detection system agent installed in either Dom 0 in each cloud server. It analyzing the VMs in server like any vulnerability is present or not it is more efficient to scan the traffic in Dom0 because all traffic in the cloud server needs go through it. The agent is implemented using snort which is mainly used for intrusion detection and prevention system. The agent is more important than compared other process present in the system.

- **Attack analyzer:**

The process of constructing and utilizing the SAG consists of three phases: Information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modeled using SAG. Each path from an initial node to a goal node represents a successful attack.

- **Network Controller:**

The network controller is a keycomponent to support the programmable networking capability to realize the virtual network reconfiguration feature based on Open Flow protocol. In NICE, within each cloud server there is a software switch, for example, OVS, which is used as the edge switch for VMs to handle traffic in and out from VMs. The network controller is responsible for collecting network information of current attack graphs the information includes current data paths on each switch and detailed flow information associated with these paths, such as TCP/IP and MAC header. The network flow and topology
change information will be automatically sent to the controller and then delivered to attack analyzer to reconstruct attack graphs.

- **VM Profiling:**

It is acting as a database in the NICE system. It carried out all .information like state, ports, and services running and also contains comprehensive information like vulnerabilities, alert, and traffic. The information are comes from Attack graph generator, NICEA, Network controller.

- **Performance Evaluation:**

The system performance of NICE system evaluated based on the process of CPU utilization, Communication delay, Traffic load. In NICE system implemented in server cluster.

VI. System Implementation

The cloud user successfully stored data in the Virtual machine. Then the cloud server consist all the data which is stored by cloud user. From the server side scans each time when the user comes stored in particular VM. If any intruder modifies any data means it will sent alert message to a particular cloud user Countermeasures Selection[9] are initiated by the attack analyzer based on the evaluation results from the cost-benefit analysis of the effectiveness of countermeasures. Then, the network controller initiates counter measure actions by reconfiguring virtual or physical Open Flow switches. [9] After the NICE-A analyze the attack and Attack analyzer construct an attack graph to provide information about which VM consist vulnerability then it send to Network Controller to provide appropriate counter measures and block the particular attacker in the cloud server. Countermeasure such as Network reconfiguration, Traffic redirection, IP address change for analyzing reach packet and block a particular VM in a server change the IP address.

Algorithm: Countermeasure_Selection
Require: Alert;G(E,V); CM
1: Let vAlert = Source node of the Alert
2: if Distance to Target vAlert > threshold then
3: Update ACG
4: return
5: end if
6: Let T = Descendant vAlert U vAlert
7: Set Pr(vAlert) = 1
8: Calculate_Risk_Prob(T)
9: Let benefit[|T|.|CM|]=0
10: for each t do
11: for each cm < CM do
12: if cm<condition then
13: Pr(t) = Pr(t)*(cm:effectiveness)
14: Calculate_Risk_Prob(Descendant(t))
15: benefit[t, cm]=Pr(target node).
16: end if
17: end for

18: end for
19: Let ROI{|T|; |CM|=0 ;
20: for each t < T do
21: for each cm< CM do
22: end for
23: end for
24: Update SAG and Update ACG
25: return Select Optimal CM (ROI)

VII. Conclusion

In this paper, we presented 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 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. NICE only investigates the network IDS approach to counter zombie explorative attacks. In order to improve the detection accuracy The attacks are prevented in the multiple server cluster to provide a counter measures. For purpose of reducing false alert using alert correlation graph investigated as future work.

REFERENCES

[1] NICE https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6419708
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A.Konwinski,G. 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.
[3] B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," *IEEE Int'l Conf. Computer Communication and Informatics (ICCCI '12)*, Jan. 2012.
[4] 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.
[5] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker,"Detecting spam zombies by monitoring outgoing messages," *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 2, pp. 198–210, Apr. 2012. IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING
[6] 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.
[7] G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," *Proc. of 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08)*, Feb. 2008.
[8] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," *Proc. IEEE Symp. on Security and Privacy*, 2002, pp.273–284.
[9] "Open flow." http://www.openflow.org/wp/learnmore/, 2012.
[10] http://www.researchgate.net/publication/222409606_Using_attack_ correlating_hypothesizing_and_predicting_intrusion_alerts

MadhuSudan.S completed B.E (ISE) from APS College of Engineering Bangalore, Karnataka in 2011 and pursuing M.Tech (CSE) in MVJ College of Engineering Bangalore, Karnataka. His main research interests include Cloud Computing, Network Security and Wireless Communication.

Srikanth SP is a Computer Science Engineer, presently working as an Associate Professor in the department of Computer Science & Engineering of MVJ College of Engineering, Bangalore. He pursued his M.tech from VTU and B.E from Mysore University .He has total 5 and counting more paper publications in journals and conferences (National & International).