Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.36 – 40

RESEARCH ARTICLE

SECURE NETWORK COMMUNICATION AND INTRUSION DETECTION IN VIRTUAL MACHINES

Tejashree A Rahane[1], Raksha S Wani[2], Gayatri D Kute[3], Monika V Deore[4]

Final Year, Computer Engineering, S.V.I.T. Nashik, Pune University, India

[1] tejashreerahane@gmail.com

[2] pinky131993@gmail.com

[3] kutegauri11@gmail.com

[4] monikanjali@gmail.com

Abstract— Cloud computing is becoming one the fastest growing field in the information technology. cloud computing allow us to scale our server in magnitude and availability in order to provide service to greater number of end user .In recent year cloud security is being seen as point of attraction for many research centers. The attackers may investigate the susceptibility to attack, the cloud system which consist of virtual machine that may unfold to large scale DDOS(Distributed Denial of service). In cloud system the detection of zombies attack detection is extremely difficult. Intrusion & prevention system (IDPS) are used to identify possible attacks, collecting information about them & then trying to stop their occurrence & at last reporting them to system administrator. These system are used by some organization to detect the weakness in their security policies, documenting existing attack and threats & preventing an individual from violating security policies.

Because of their advantages these system became an important part of security infrastructure in nearly every organization. To avert these virtual machine from argument. Therefore a multi phase solution is been developed.

Keywords— Cloud Security, Zombie Attack Detection, Cloud Computing

I. INTRODUCTION

Distributed Denial of Service is a type of attack that aims to make services or resources unavailable for indefinite amount of time by flooding it with unwanted traffic. The main objectives of these attacks are, to exhaust computer resources (CPU time, Network bandwidth) so that it makes services unavailable to legitimate users. In a general DDoS attack, the attacker usually disguises or 'spoofs' the IP address section of a packet header in order to hide their identity from their victim. This makes it extremely difficult to track the source of the attack. IP trace back is a scheme that provides an effective way to trace the Source of DDoS attacks to its point of origin. What makes this more disastrous is that it is extremely difficult to selectively filter the malicious traffic without impacting the service as a whole.

II. EXISTING SYSTEM

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).

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.

Disadvantages of Existing System

- No detection and prevention framework in virtual networking environment
- No Accuracy in Attack detection From attackers.

III. PROBLEM DEFINATION

We develop devise 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. NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services. NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.

NICE optimizes the implementation on cloud servers to minimize resource consumption. Our study shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions. NICE significantly advances the current network IDS/IPS solutions by employing programmable virtual networking approach that allows the system to construct a dynamic reconfigurable IDS system. By using software switching techniques , NICE constructs a mirroring-based traffic capturing framework to minimize the interference on users' traffic compared to traditional bump-in-the-wire (i.e., proxy-based) IDS/IPS. The programmable virtual networking architecture of NICE enables the cloud to establish inspection and quarantine modes for suspicious VMs according to their current vulnerability state in the current SAG. Based on the collective behavior of VMs in the SAG, NICE can decide appropriate actions, for example, DPI or traffic filtering, on the suspicious VMs

IV. PROPOSED METHODOLOGY

There by preventing zombies virtual machine. To make a firm defense in depth intrusion detection framework, we propose a system for better detection of attempt to damage. The system ensures the attack graph analytical procedures in intruding the detection processes. The structure of NICE is not made to improve any of the existing intrusion detection algorithms but rather it helps to reconfigure the virtual networking attempt for detection and applying counter to compromise.

1 NICE (Network Intrusion detection and Countermeasure Selection in virtual network systems) is proposed to establish a defense-in-depth intrusion detection framework.

2 For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes.

3 The design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

4 Deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability towards the collaborative attack goals, NICE will decide whether or not to put a VM in network inspection state.

5 Once a VM enters inspection state, Deep Packet Inspection (DPI) is applied, and/or virtual network reconfigurations can be deployed to the inspecting VM to make the potential attack behaviors prominent.

6 By using software switching techniques, NICE constructs a mirroring-based traffic capturing framework to minimize the interference on users' traffic compared to traditional bump-in-the-wire (i.e., proxy-based) IDS/IPS.

7 NICE enables the cloud to establish inspection and quarantine modes for suspicious VMs according to their current vulnerability state in the current SAG.

8 Based on the collective behavior of VMs in the SAG, NICE can decide appropriate actions, for example DPI or traffic filtering, on the suspicious VMs. Using this approach, NICE does not need to block traffic flows of a suspicious VM in its early attack stage.

Advantages Of Proposed system

- NICE significantly advances the current network IDS/IPS solutions by employing 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.
- NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services.
- NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.
- NICE optimizes the implementation on cloud servers to minimize resource consumption. Our study shows that NICE consumes less computational overhead compared to proxy-based network intrusion.

V. SYSTEM ARCHITETURE

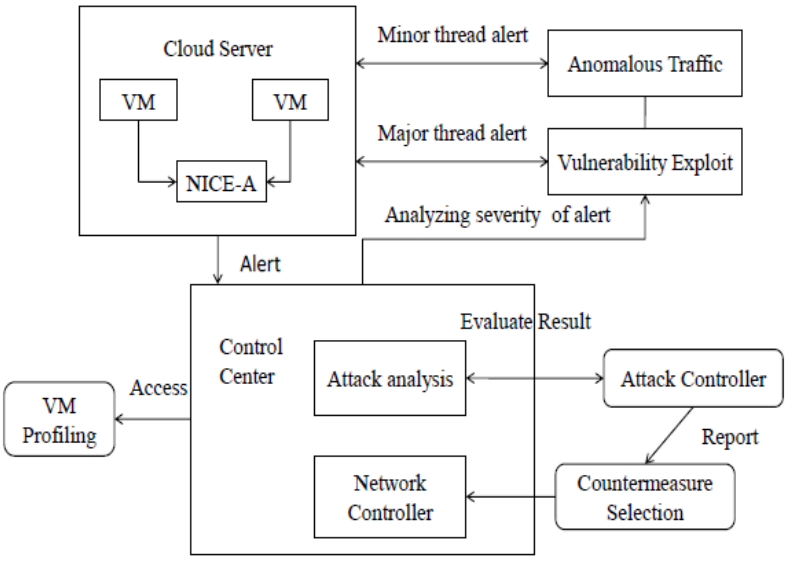

Fig. System Aechiteture

The NICE framework within one cloud server cluster. Major components in this framework are distributed light-weighted NICEA 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. The architecture of NICE system explains complete prevention of zombie exploration by the intruders by taking countermeasures by intruders.

- **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 on-premises servers.

- **Cloud User**

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 on-premises servers.

- **NICE-A**

The NICE-A is a network intrusion detection system (NIDS) 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 key component 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, NICE-A, 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 Dom 0 level in server cluster. So, the performance is evaluated how the vulnerabilit identified in this level when compared to proxy based and Dom U level.

VI. CONCLUSIONS

In this paper we are proposing a system for detecting and reducing attack in cloud environment. so that the cloud service provider permits the authenticate cloud user to access then the cloud user stores the file in virtual machine as enc encrypted format successfully. From the server side scans every time when user access their files. The vulneravibility to be detected and prevented using multiphase distributed mechanism in multiple server clusters**.** The attacks are prevented in multiple server cluster to provide a countermeasure.

ACKNOWLEDGEMENT

We would particularly like to thank Prof. M.M Naoghare for stimulating discussion that we had And also we thank for her valuable suggestions**.**

REFERENCES

[1] Coud Sercurity Alliance, "Top Threats to Cloud Computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, Mar. 2010.
[2]B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.
[3] H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.
[4] 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.
[5] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi,"Securing cloud computing environment against ddos attacks"International Conference on Communication, Volume 5.
[6] Bhaskaran M., Natrarajan.A.M. and Sivanandam. S.N.,(2007),"Trace Backing the Spoofed IP Packets in Multi ISP Domains with"Secured Communication," IEEE-ICSCN 2007, pp 579-584.
[7]Chun-jen chun, Pankaj khatkar,Tianyi Xing, NICE: Network intrusion detection and countermeasure selection in virtual network system IEEE TRANSACTION ON DEPENDABLE AND SECURE COMPUTING,VOL.10,NO.4,JULY/AUGAST 2013

