Host Based Intrusion Detection to Prevent Virtual Network System from Intruders in Cloud

J. Sasi Devi[1], R. Sugumar[2]

[1] Research Scholar, St.Peter's University, Chennai, India

[2]Associate Professor, Veltech Multitech Engineering College, Chennai, India

Abstract: ***In Cloud System, virtual machine is considered as the security threat. This is because all cloud users install their applications in virtual machines. 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 multiphase distributed vulnerability detection measurement and countermeasure selection mechanism. It built an attack graph analytical model which is used for identify the intruders possible way of exploit vulnerability. The model consist information about virtual topology and also about cloud servers. Based on the information provided by the analytical model then the system deploy an appropriate counter measures.***

Keywords: Cloud Server, DDOS, Intruders, Virtual machine, Vulnerability

1. Introduction

In traditional data centers, where system administrators have full control over the host machines, vulnerability 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 a can violate the service level agreement (SLA). 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 of its resource to deploy attacks in more efficient ways. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, and so on, attracts attackers to compromise multiple VMs.

In this paper, proposing Network Intrusion detection and Countermeasure sElection in virtual network systems (NICE) to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs. It includes two main phases: 1) 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). 2) Once a VM enters inspection state, deep packet inspection is applied. The contribution which is involved in NICE system is (i) the framework of the system that captures and inspects suspicious cloud traffic without interrupting user's applications and cloud services (ii) Improving the attack detection probability and improves the resiliency to VM exploitation attack without interrupting existing normal cloud services. (iii) It employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures. (iv) It consumes less computation overhead compared to other intrusion detection solutions.

a) Attack Graph Model

An attack graph is a modeling tool to illustrate all possible multistage, multi host attack paths that are crucial to understand threats and then to decide appropriate countermeasure. In attack graph, each node represents either precondition or consequence of an exploit. The actions are not necessarily an active attack because normal protocol interactions can also be used for attacks. Attack graph is helpful in identifying potential threads, possible attacks, and known vulnerabilities in a cloud system.

b) Thread Model

In attack model, assume that an attacker can be located either outside or inside of the virtual networking system. The attacker's primary goal is to exploit vulnerable VMs and compromise them as zombies. The protection model focuses on virtual-networking-based attack detection and reconfigurable solutions to improve the resiliency to zombie explorations. The cloud service users free to install whatever operating systems or applications they want, even if such action may introduce vulnerabilities to their controlled VMs.

2. Related Works

Z.Duan, P.Chen, F.Sanchez "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. So, 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 are recognized as one

of the most serious security threats. In contrast to previous malware, botnets have the characteristics of a command and control (C&C) channel. This makes the detection of bonet C&C a challenging problem. It proposing an approach that uses network-based anomaly detection to identify botnet C&C channels. O.Sheyner, 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, A.vijayan "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). So, proposing a quantitative solution for analyzing alerts generated by the IDSs, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the FTA for the flooding attacks. P.Ammann, D.Wijesekera "Scalable, graph based network vulnerability analysis", A variety of graph-based algorithms to generate attack trees (or graphs).Either structure can take advantage of the penetration achieved by prior exploits in its chain and the final exploit in the chain achieves the attacker's goal. G.Gu, P.Porras, V.Yegneswaran, M.Fong, and W.Lee "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, 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 well-guarded 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.

3. Back Ground

In Cloud environment, the virtual machines are an important factor. An attacker can explore vulnerability of a cloud system and compromising virtual machines. DDOS (Distributed Denial of Service) attacks usually involve early stage actions such as multistep exploitation, low-frequency vulnerability scanning and compromising identified vulnerable virtual machines as zombies, and finally DDOS attacks through the compromised zombies. Within the cloud system, especially the infrastructure as a service (laas) clouds, the detection of zombies exploration attacks is extremely difficult.

4. System Architecture

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

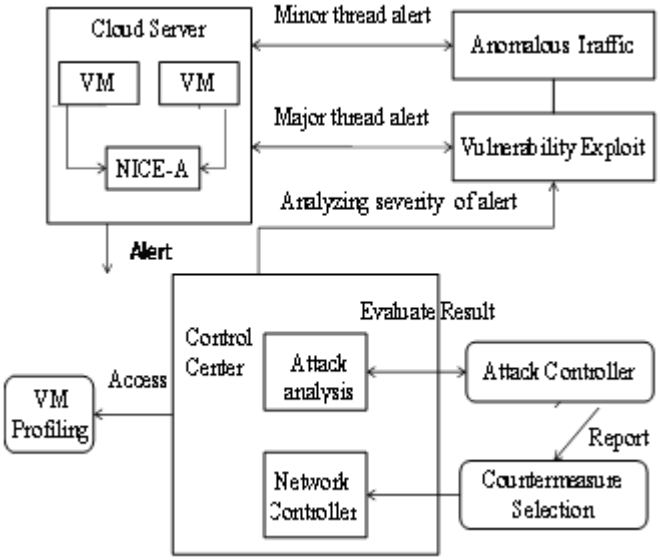

Figure 1: System Model

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.

5. 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 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 system. 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 on-premises servers.

Cloud User:-The provider allows an authenticated user to 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 (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 vulnerability identified in this level when compared to proxy based and Dom U level.

6. 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. 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. Network reconfiguration denotes that configuring the settings of Particular virtual machine. The anomalous traffic raised by attacker means automatically transfers the data from one VM to another VM. Topology setting changed by the intruders means it takes packet filtering countermeasure 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)

7. Conclusion and Future Work

In conclusion, the cloud service provider permits the authenticated cloud user to access. Then, the cloud user stores the file in a virtual machine as encrypted format successfully. From the server side scans every time when users access their files. The vulnerability to be detected and prevented using multiphase distributed mechanism in multiple server clusters. 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] Cloud Security Alliances, 2010"Top Threats to Cloud Computing v1.0.
[2] Armbrust.M, Fox.A, Griffith.R, Joseph.A.D, Katz.R, Konwinski.A, Lee.G, Patterns.D, 2010"A View of Cloud Computing," ACIM Comm., vol.53, no.4, pp.50-58.
[3] B.Joshi, A.Vijayan, and B.Joshi, 2012"Securing Cloud Computing Environment against DDOS Attacks,"Proc.IEEE Int'f Conf Computer Comm. And Informatics (ICCCI'12).
[4] H.Takabi, J.B.Joshi,and G.Ahn,2010"Security and privacy Challenges in Cloud Computing Environment," IEEE Security and Privacy, Vol.8, no.6,pp.24-31.
[5] "Open vSwitch Project," May 2012.
[6] Z.Duan, P.Chen, F.Sanchez, Y.Dong, M.Stephenson,and J.Barker,2010"Detecting Spam Zombies by Monitoring Outgoing Messages,"IEEE Trans,Dependable and Secure Computing, vol.9, no.2,pp.198-210.
[7] G.Gu, P.Porras, V.Yegneswaran, M.Fong, and W.Lee,"BotHunter:Detecting Malware Infection through IDS-driven Dialog Correlation," Proc.16th USENIX Security Symp.(SS'07).
[8] G.Gu, J.Zhang, and W.Lee, 2008"Botsniffer: Detecting Botnet Command and Control Channels in Network Traffic,"Proc.15th Ann.Network and Distributed System security Symp.(NDSS'08).
[9] O.Sheyner, J.Haines, S.Jha, R.Lippmann, and J.M.Wing, 2010"Automated Generation and Distributed Symp. (NDSS'08).
[10] "NuSMV:A New Symbolic Model Checker,/nusmv.Aug 2012.
[11] O.Database,"Open Source Vulnerability Database (OVSDB)," 2012.
[12] A.Roy, D.S Kim, and K. Trivedi, 2012" Scalable optimal Countermeasure Selection Using Implicit Enumeration on Attack countermeasure Trees," Proc.IEEE Int'I Conf.Dependable Systems Networks (DSN'12).
[13] N.Poolsappasit, R.Dewri, and I.Ray,2012"Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans.,Dependable and secure computing, vol.9,no.1,pp.61-74.
[14] National Institute of standards and Technology, 2012"National Vulnerability Database, NVD," http://nvd.nist. Gov.
[15] "Metasploit, 2012" http:// www.fastandaesyhacking.com.