SECURE AND IMPLEMENTATION OF INTRUSION DETECTION IN VIRTUAL MACHINE SYSTEMS

[1]U.Murugan, [2]Guru Rama Senthilvel

Abstract – Cloud protection is one of better essential argument that have fascinated a lot of examine and improvement struggle in past few years. Mainly attackers can examine vulnerabilities of a cloud structure and adjustment virtual machinery to organize further large-scale Distributed Denial-of-Service (DDoS). DDoS intrusion usually involve early stage performance such as multi-step 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 (IaaS) clouds. In the cloud system, the detection of zombie exploration attacks is particularly complicated. This is because cloud users may install vulnerable applications on their virtual machines. Attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). In the proposed system, Cloud Server will analyze each data that was uploaded in the Cloud Server. There is an access control mechanism to analyze the content of the data already stored in a server. it is not possible for an attacker to fetch the malicious content to perform malicious activities. The challenge is to authorize an efficient vulnerability/attack detection and response structure for accurately identifying attacks and minimizing the impact of security to cloud users.

Keywords -- Network security, cloud computing, intrusion detection, attack graph, zombie detection

----

I. INTRODUCTION

In conventional records centers, where structure administrators have full control over the host machines, vulnerability can be recognize and reconstructed by the structure administrator in a centralized manner. However, reconstructing is known as protection holes in cloud records centers.

- ***Murugan.U** is currently pursuing masters degree program in computer science engineering. Ph-9094965955.*
- ***Guru Rama Senthilvel**, M.E., A.P/ HOD of IT Dept, Ph-98410 65075*

The cloud users frequently have the benefit to control software installed and managed VMs, may not work efficiently and a can break the service level agreement (SLA). In a cloud system, where the transportation is shared by possible millions of users, abuse and nefarious use of the shared transportation profit attackers to accomplish vulnerabilities of the cloud and use of its reserve to deploy attacks in more powerful ways. The related setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software; structure, and so on, attackers to adjustment of many VMs.

Botnets are different from other forms of attacks such as clone in that they use command and control (C&C) channels. It is significant to study this botnet characteristic so as to expand efficient countermeasures. Moreover, the exposure of the C&C channel will reveal both the C&C servers and the bots in a directed structure. Therefore, accepting and identifying the C&Cs has great value in the battle against botnets.

A. Distributed Denial of Service (DDOS)

Distributed denial of service intrusion on origin name slavers of an Internet events in which distributed denial-of-service intrusion object in one or more of the thirteen Domain Name scheme and source name slavers clusters. The source name slavers are demanding infrastructure machinery of the Internet, checking domain names to Internet Protocol (IP) location and other source record (RR) data. Attacks against the root name servers could, in theory, contact operation of the whole universal Domain Name System, and thus all hyperspace services that use the universal DNS, rather than just particular websites. However, in practice, the origin name slave infrastructure is highly flexible and spread using both the natural quality of DNS (result caching, retries, and multiple servers for the equivalent zone with fallback if one or more fail), and, in recent years, a grouping of any cast and load balancer routine used to execute most of the thirteen nominal individual origin slave as universally spread clusters of slave in many records centers.

II. RELATED WORKS

2.1 LITERATURE SURVEY

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 frequently used to launch various protection intrusion 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 efficient spam zombie finding structure named SPOT by monitoring leaving messages of a institute.

G.Gu, J. Zhang "BotSniffer: Detecting Bonet command and Control channels in Network traffic", Bonets are recognized as one of the most serious protection pressure. This technique is to distinguish the earlier 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 essential part of modeling the universal view of system protection 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 recognizing and searching the distributed denial of service (DDOS) intrusion in cloud computing surroundings. This type of intrusion is repeatedly the source of cloud utility interruption. The solution is to combine the evidences obtained from intrusion detection systems (IDSs). So, proposing a quantitative result for searching signals are accomplish 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 progress to growth a immediate source for browsing the distributed denial-of-service (DOS) activities and direct attacks, catching position across the Internet. Among the many forms of malicious software, botnets in exacting have freshly determined themselves to be along with the leading threats to computing assets. Like the previous generations of computer viruses and worms, a bot is a self-generating relevance that affect the vulnerable manager over straight utilization or Trojan insertion. All bots distinguish themselves from the other malware forms by their capability to provide a command and control (C&C) path over which they can be informed and focussed Once collectively under the control of a C&C server, bots structure what is introduced to as a botnet.

L.Wang, A.Liu and S.jajodia, "Using Attack graphs for Correlating, Hypothesizing and Predicting Intrusion 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-established unfocused in Intrusion Detection Systems (IDSs). That is, sharp information 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.

2.2 BACKGROUND

In cloud environment, the virtual machines are an important factor. An Attacker can explore a vulnerability of a cloud system and compromising virtual machines. DDoS (Distributed Denial of Service) attacks usually involve early stage actions such as many-stride accomplishment, low-density vulnerability browsing, and dealing the identified vulnerable essential machines as zombies, and finally DDoS attacks over the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the finding of zombie exploration intrusion is highly different.

The machinery is to detect and preventing a vulnerable virtual machines in cloud. NICE implemented in a one server cluster to prevent the suspicious virtual target from intruders. It builds an attack analytical model to discover the intruder's vulnerability and information about a possible way of exploit and deploy appropriate countermeasures.

.A. NICE-A

It browse the traffic going over the bridges that control all traffic among VMs and in/out from the cloud servers.

B. VM Profiling

This will monitor the knowledge about any open ports on a VM and the past of released harbors cooperates a significant role to a network controller. All these factors combined will form the VM profile.

C. Attack Analyzer

It contain of three part of gathering the Information, Attack Graph Model and Exploit path analysis. Attack path can be modeled as SAG(Scenario Attack Graph).

D. Network Controller

If a ruthless wired is tracker and establish a quantity of known attacks, or a Attack Analyzer is detected as a DoS attacks, then the NC will block to download that data.

III. PROPOSED SYSTEM

Cloud server will analyze each new data that was uploaded in the cloud server. There is an access control mechanism to analyze the content of the data already stored in a server.

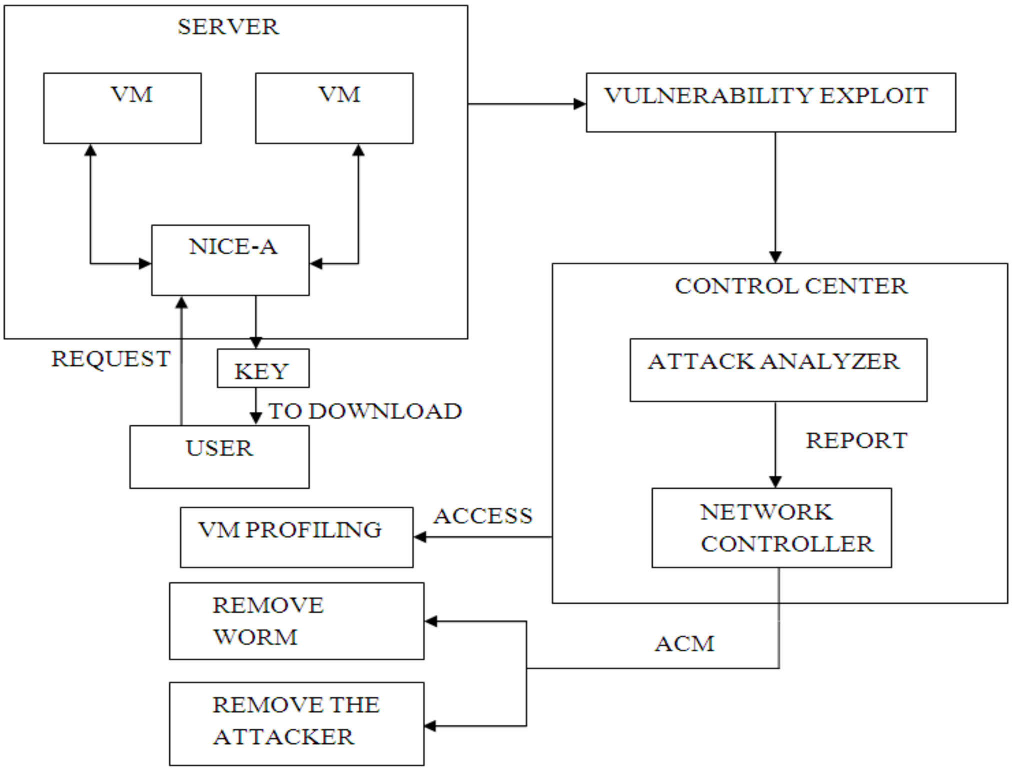

Fig 1. Overall Architecture of cloud server

The cloud server is not possible for an attacker to fetch the malicious content to perform malicious activities. If the data packets contain the malicious data, then the server will detect the concerned node and remove the node from network .If user download data from server, only authorized user can download data after entering a correct key. . If any malicious detected, then the server will remove only malicious node. It is efficient for finding detection and prevention in a cloud system. In fig.1 describe the overall system.

The NICE (Network Intrusion Detection and Counter measure Selection) fig 1 framework within one cloud server. Major components in this framework are scattered and light-weighted NICE-A on each objective cloud slave, a set of connections organizer, a VM profiling slave, and an intrusion analyzer. The last three mechanism are positioned in a centralized organizer coupled to software switches on every cloud slave (i.e., virtual switches built on one or many Linux software bridges).The association organizer is dependable for expanding attacks in countermeasures based on compromises made by the intrusion analyzer.

A. Data Authorization And Authentication.

The provider allows an authenticated user to allow accessing a server for storing or retrieving a file or any data. It can be profiled to get information about their state, service running and contain information about vulnerability and traffic. It scans the traffic going through bridges that control all the traffic among VMs and in/out from servers.

Virtual equipment in the cloud can be generalised to get precise instruction about their state, services running, open ports, and so on. One chief reason that counts againts a VM profile is its related with previous VMs. Any VM that is connected to more number of machines l. In this module VM-profiling is used store the information about the incoming request of the cloud user the information like port no ,ip address and Mac address and few information .this information is used to check the continues request done by the cloud server.

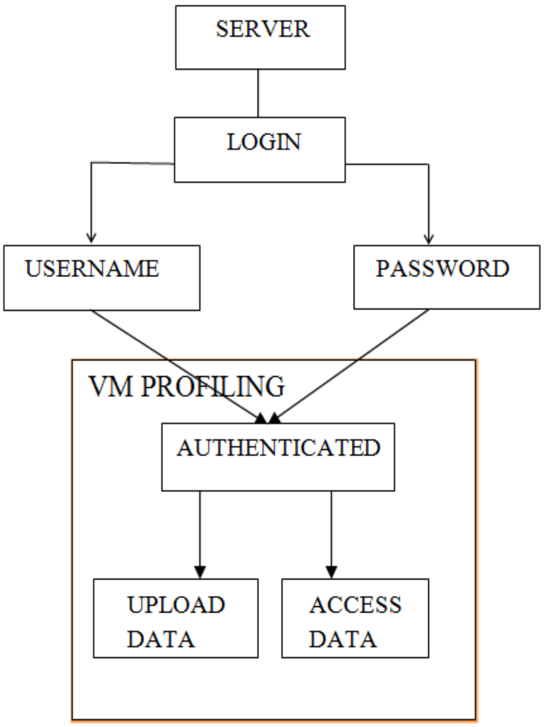

Fig 2. Data Authorization and Authentication.

B. Intrusion Detection Using Alert Correlation Algorithm

The major functions of NIDS are performed by attack analyzer and network controller. NIDS includes attack graph model, alert correlation which is based on attack analyzer. It checks whether the data send by the nice agent has any attack by comparing with the data base in the previous history. Phases: Information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modelled.

Each join in the intrusion graph perform an utilize by the attacker. Each way from an primary node to a ambition node perform a successful attack. We can have traffic pattern, where packets emanate from a single IP and are hand over the many destination IP addresses, and vice versa. The association manager that allows the cloud structure to set security/filtering rules in an integrated and comprehensive manner. If an attack is severe and identifies the VM which is detected as a zombie, then the network controller will block VM immediately in fig 3.

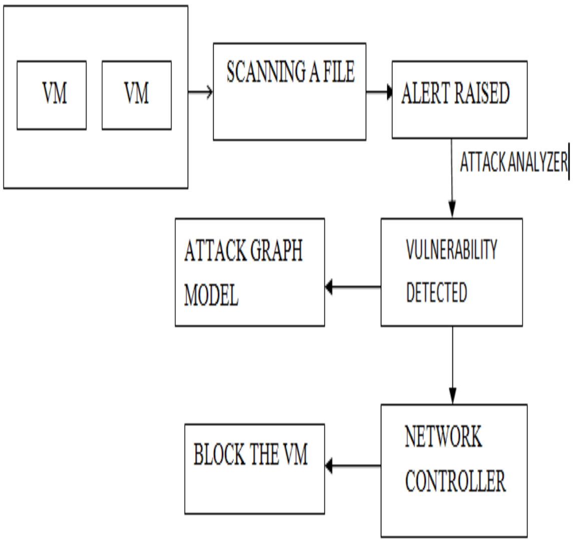

Fig 3. ***Intrusion Detection Using Alert Correlation Algorithm***

Algorithm 1: Alert correlation

```
alert ac, SAG, ACG
S:if (ac is a new alert) then
create node ac in ACG
n1 ← vc € map(ac)
for all n2 € parent(n1) do
create edge (n2.alert, ac)
for all Si containing a do
if a is the last element in Si then
append ac to Si
else
create path Si+1= {subset(Si,a),ac}
end if
end for
add ac to n1.alert
end for
end if
return S
```

C. Data Encryption

If user upload any malicious data or do any attacks in virtual machine data, then find out the specified user and remove that user from the server. When user continuously giving request to same file for downloading, the server will consider as anonymous user and block the user immediately.

D. Secret Code Data Retrieval

Server will provide the secret key to authorized user for upload and download the data from server. Secret key is generated by using DES(Data Encryption Standard) algorithm. If user want to download any data from server, user will enter the correct key to download the data.

IV. RESULT ANALYSIS

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.

The information provide 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. Data authorization and authentication 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.

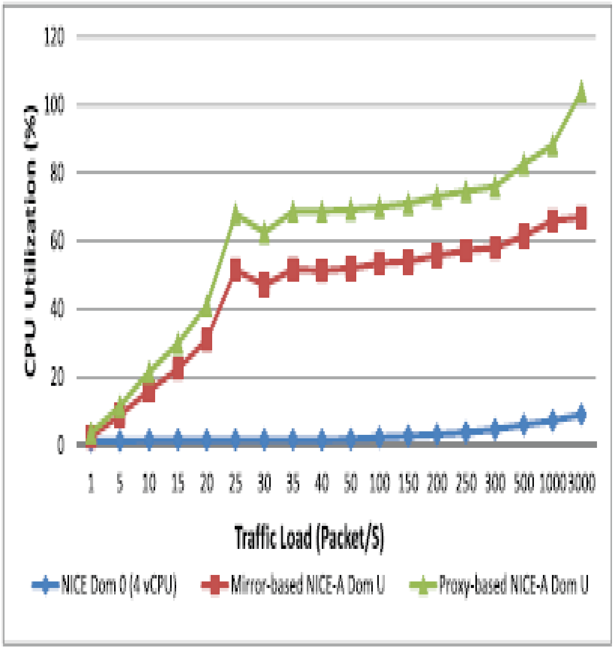

Fig 4. ***CPU Utilization vs Traffic Load***

V. CONCLUSION

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.

VI. REFERENCES

[1]Cloud Security Alliances, “Top Threats to Cloud Computing v1.0,”http://clouds security alliances.org/top threats. v1.0.pdf, Mar.2010

[2]M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz, A.Konwinski, G.Lee, D.Patterns ,”A View of Cloud Computing,” ACIM Comm., vol.53,no.4,pp.50-58,Apr.2010

[3]B.Joshi, A.Vijayan, and B.Joshi,”Securing Cloud Computing Environment against DDOS Attacks,”Proc.IEEE Int’f Conf Computer Comm. And Informatics(ICCCI’12), Jan 12.

[4]H.Takabi, J.B.Joshi,and G.Ahn,”Security and privacy Challenges in Cloud Computing Environment,” IEEE Security and Privacy, Vol.8, no.6,pp.24-31, Dec.2010.

[5]”Open vSwitch Project,” http://openvswitch.org,May 2012.

[6]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.

[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,”Botsniffer:Detecting Botnet Command and Control Channels in Network Traffic,”Proc.15th Ann.Network and Distributed System security Symp.(NDSS’08),Feb.2008.

[9]O.Sheyner, J.Haines, S.Jha, R.Lippmann, and J.M.Wing,”Automated Generation and Distributed Symp.(NDSS’08),Feb.

[10]”NuSMV:A New Symbolic Model Checker,”http://afrodite.itcit.1024/nusmv.Aug 2012.

[11]O.Database,”Open Source Vulnerability Database(OVSDB),” http://osvdb.org/,2012.

[12]A.Roy, D.S Kim, and K. Trivedi,” Scalable optimal Countermeasure Selection Using Implicit Enumeration on Attack countermeasure Trees,” Proc.IEEE Int’l Conf.Dependable Systems Networks(DSN’12),June 2012.

[13]N.Poolsappasit, R.Dewri, and I.Ray,”Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Trans.,Dependable and secure computing, vol.9,no.1,pp.61-74,Feb.2012.

[14]National Institute of standards and Technology,”National Vulnerability Database, NVD,” http://nvd.nist. Gov, 2012

[1]Murugan.U received degree B.E Computer Science and Engineering from Kings Engineering College, Anna university in 2012. Now pursuing M.E Computer Science and Engineering in Meenakshi College of Engineering, Anna university, Chennai. Ph- 9094965955.

[2]Guru Rama Senthilvel received B.Sc., (Physics) from Madurai Kamaraj University in 1992, MCA., from Madurai Kamaraj University Campus in1996 and M.E (CSE) from Anna University, 2007. Currently,he is the Head of the department in Information technology.Ph-9841065075.