Host Based Network Intrusion Detection System in Virtual Machine

Rupali Pravin Adhau[1], Saba Siraj[2]

[1]Savitribai Phule Pune University, Institute of Knowledge COE, Pune, India

[2]Professor, Savitribai Phule Pune University, Institute of Knowledge COE, Pune, India

Abstract: ***Cloud computing gaining popularity in the recent era.In past few year security is the main issue in the cloud computing. Intrusion Detection and Prevention Systems (IDPS) is mainly used: to identify possible attacks, collect all information about that attack and finally give this information to the system administrator. The IDS is used to detect the security level in many organizations. In a Cloud computing, attackers can find the vulnerabilities in the cloud systems and compromise the virtual machines to set out large scale Distributed Denial-of-Service (DDOS) attack. This is very difficult to avoid this attack in the cloud computing environment. To prevent vulnerable virtual machines from being compromised in the cloud computing, I have proposed a multi-phase distributed vulnerability detection, measurement, and countermeasure (NICE). (Network Intrusion Detection and Countermeasure selection in Virtual Network Systems)***

Keywords: Network Security, Cloud Computing, Intrusion Detection, Attack Graph, Zombie Detection, Denial of service.

1. Introduction

In the recent years it have been seen that the no of user migrating toward the cloud are facing main issue of the security. The survey says that cloud computing is most vulnerable to the security. in the cloud computing attackers can explore vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In the existing system data is store on the one central machine and administrators have full control of that virtual machine. So that in this system attack can be detect and control by system admin only. In the cloud computing system end user can install any software on their virtual machine which may lead to the violation in the cloud security. The challenge in cloud computing is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and also minimizing the effect of that attack on security breach to cloud users. In the cloud computing large infrastructure is shared by the number of user across the world. That is the reason attackers use this infrastructure to deploy the any attack on the cloud. Because cloud users mainly uses same cloud resources such as hub, switches, adapter in common. These users are also use same data storage and file system, now a days common virtual machines VM OS installed, different software, networking are also shared among the users. All this things are attract to the attackers to compromise the multiple virtual machines.

In this article we have proposed novel intrusion detection system in cloud computing titled as NICE (Network Intrusion detection and Countermeasures in VM network systems) which helps to better detection of the attacks on the cloud and helps to prevent the zombie VMs attack.

In general NICE comprises of two main phases: One of them is Deploy the intrusion detection agent (NICE A) on each cloud server which mainly helps to capture and analyze the traffic. NICE Agent periodically scan the virtual machine on the cloud server and maintain the Scenario Attack Graph (SAGs). Then according the identified vulnerabilities towards the attack and then NICE will decide to put this VM in network inspection or not.(2) If VM is entered in the inspection state then Deep packet inspection is applied on that VM and virtual network reconfiguration is applied to the virtual machine which inspect the prominent attack in the network.

NICE is advances than current IDS and IPS that it allow the dynamically reconfigurable network IDS By using the software switching methods nice uses mirror based traffic monitoring system in which there is less interference on user traffic as compared to the existing (Proxy based)IDS. The programmable virtual network enables cloud to inspecting mode and quarantine mode for the suspected VM in the network using this approach nice doesn’t need to avoid traffic to the VM in the initial stage.

We have proposed a novel framework NICE network detection and preventation that capture the virtual network traffic and monitor the suspected VM and avoid intrusion without interrupting the user applications and cloud services.

NICE introduce the software switching technique that monitor and inspect the suspicious VM for further investigation and protection. By using the programmable software nice can improve the intrusion detection probability without interrupting existing cloud services. NICE introduces a novel attack graph approach to detect the attack and prevention by co relating attacks. The nice consumes the less resources as compared to the proxy based intrusion detection system.

2. Cloud Computing Environment

In this section we are going to see the literature on the cloud computing.[1] Michal albert explain the cloud computing. There are basic, platform as a service and software as a service, application as a service. There are two types of cloud are there one is the private cloud and another one is the public cloud. The use of cloud computing minimizes the all resources and all the resources are shared by all user of cloud.[2] the cloud computing is used by potentially millions of user. Resources are getting shared among those. The main attack in the cloud computing is the denial of service attack in the cloud. In [2] the cloud resources are transferred to the economical mode named as economical mode of denial of service. This technique determines the whether the request is coming from legitimate user or generated by the bots. In this work they have used trace back model to which is based on the deterministic packet marking algorithm. Which helps to detect the real source of the attack in the network. This system is useful to detect the denial of service attack in the ds.[3] introduces the new approaches to detect the intrusion and recognize the infection and coordination dialogue occur during the successful malware functioning. Here mainly used method is the bothunted method which bound the inbound scanning and exploit usage and egg downloading. In the last ten years malware software's and malware user are become most of the source of the denial of service attack and other malfunctioning. In this he have introduces the real time malware detection system in cloud computing. The system capabilities more as compared to other existing system.

[4] discussed about the botnet threat in the network. As compare to the previous malware the botnets have its command and control. Botnets are also used in the existing common protocol such as HTTP and other. This approaches is depends on the observation of the preprogramed activities related to the command and control. The proposed botsniffer detect the activities and find out the botnets with theoretical bounds false positives. Botsniffer introduces the uniformed behavior of the spatial virtual machine to detect the zombie by grouping the flow according to the server knowledge. [5] proposed a symbolic nuMVM checking and [6] binary decision diagram to built the binary decision graph. Their method can detect the all possible attack graph but scalability is main issue with this. Intrusion detection system and firewall is widely used to monitor and detect the suspicious activities in the network.

3. Nice Model

In this section we will see how to use the nice model to detect the intrusion in the network. The main aim of the nice is to do the vulnerable activities in the VM and avoid these activities in the network.

3.1 Threat Model

In our proposed method we have considered that attacker is located either inside or outside of the virtual networking system. The main target of the attacker is to find the vulnerable VM and compromise them as a zombie. We have introduces the new software model to resilience the exploration of the zombie. Our method does not address the host based attacks.

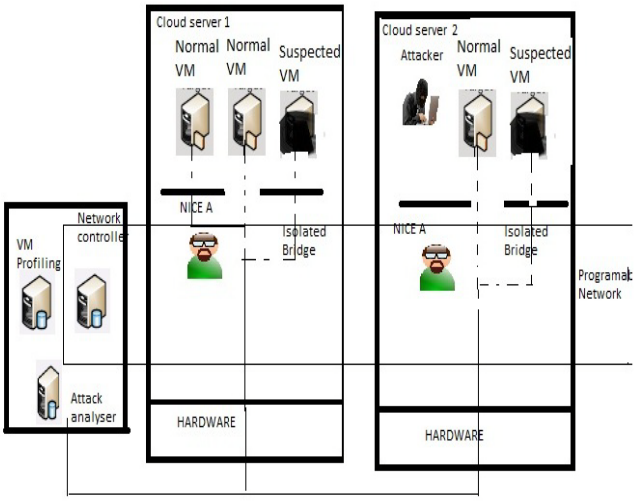

Figure 1: NICE framework

This system can be deployed on the infrastructure as a service of the cloud networking. We have assumed that the cloud service provider is being. We have as assume that the user have freedom to install the operating system whatever he wants. Physical security is out of coverage of this paper.

3.2 Attack Graph Model

Attack graph model is useful to detect all possible path to the intrusion threats and then to understand the vulnerabilities. The possible attack in the cloud system may be vulnerabilities in the cloud system. As the attack graph gives all information about the vulnerabilities and connectivity information we can get all the information by using attack graph model. If any event occurs as a attack then we can take action on that or can mitigate the attack.

```
Algorithm 1 (Alert Correlation)
Require: alert $ac$, $SAG$, $ACG$
if ($ac$ is a new alert) then
    create node $ac$
    $n1 \leftarrow vc \in map(ac)$
    for all $n2 \in parent(n1)$ do
        create edge ($n2.alert$, $ac$)
        for all $si$ having $a$ do
            if $a$ is last element In si
            then
                append $ac$ to the si
            else
                create path $Si+1 = \{subset(Si, a), ac\}$
            end if
        end for
        add $ac$ to $n1.alert$
    end for
end if
return $S$
```

5.3 Attack graph and alert correlation

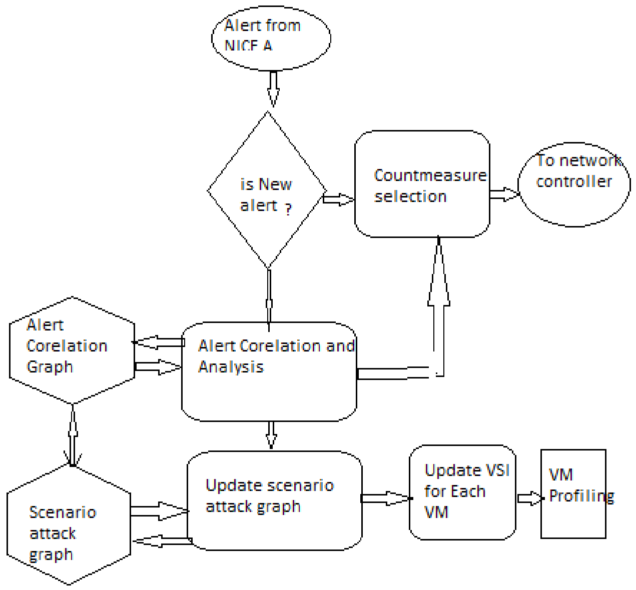

Figure 2: Flow of the NICE system Analyzer

Attack graph can be generated by using the network topologies and vulnerabilities generated in the network. To create attack graph required network knowledge and information of the running services and all vm details. This all information is provided to attack graph generator as a input. Any change in the network and in the vulnerabilities of the VM must be reflected to the graph. Attack graph is helpful to predict the attacker next steps.

4. BotHunter: Detecting Malware Infection through IDS-Driven Dialog Correlation

In the last decade the malware and malicious software are become the most important to the attack such as denial of service attack and the direct attack taking place over the internet. Same as the previous attack like worms bots is the attack which is self-propagating application which affect the vulnerable host by direct exploiting or Trojan insertion. In this paper author invented evidence-trail” approach to recognizing successful bot infections through the communication sequences which occur during the investigation process. The bots system is a bidirectional system which helps to detect and prevent the intrusion in the virtual network. The IDS system of this method is comprises of open source invented snort. It have taken full use of snort system. In addition to the snort author have design two main method which helps snort engine to produce the dialogue warning. Bothunter intrusion detection system is mainly works on the detection of the malware infection through IDS driven dialog correlation system. This system was not capable to study the total bot infection life cycle. The bothunter is the real time intrusion detection system. The bothunter attack is mainly depends on the preconditions and post conditions of the attack. Following fig shows the architecture of bothunter.

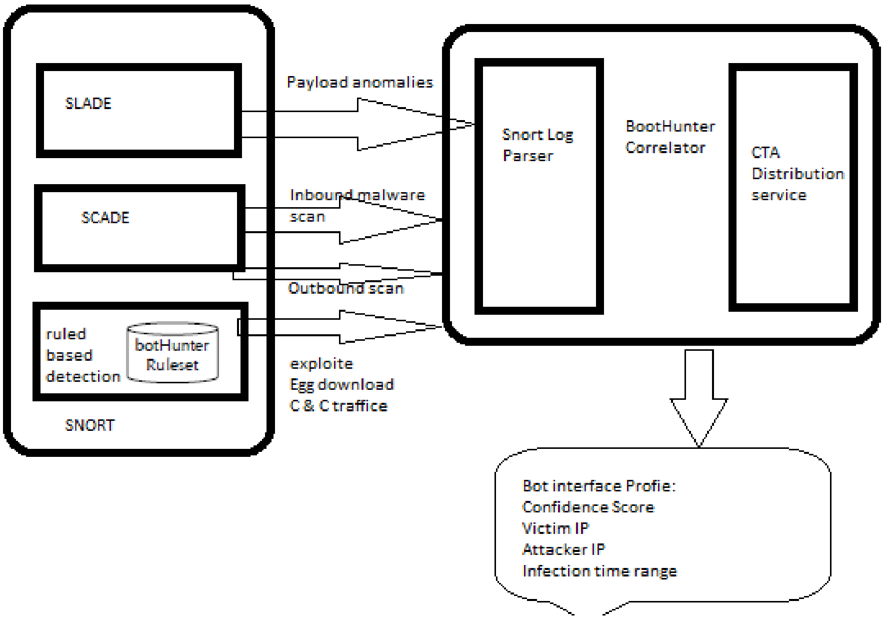

Figure 3: BotHunter Working

5. BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic

Botnets or zombies are recognized as very serious threads now a day. Botnets are total different than other kind of threads such as worms because they are using command and control channels. In this paper author have focused on the study of the botnet and then essential action to avoid the bot nets that is botmasters. The main action in this is to detect and control the command and control channel is very hardest task. In the existing mechanism all are working on the command and control channel in centralized way but in the bot sniffer it operate on the command and its response in the real time. In this paper author have studied the problem of centralized command and control channel in the network and also focuses on the two ways mechanism of the ICR and

HTTP based command channel. Botnet traffic is difficult to detect because it follows normal traffic and traffic is also same as normal traffic. In this he have studied two types of command control first is the push style and second one is the pull type where command is pull from the bots. Botsniffer is the system totally depends on the anomaly and is implemented as several plug ins. Fig 4 shows the architecture of the Bot sniffer.

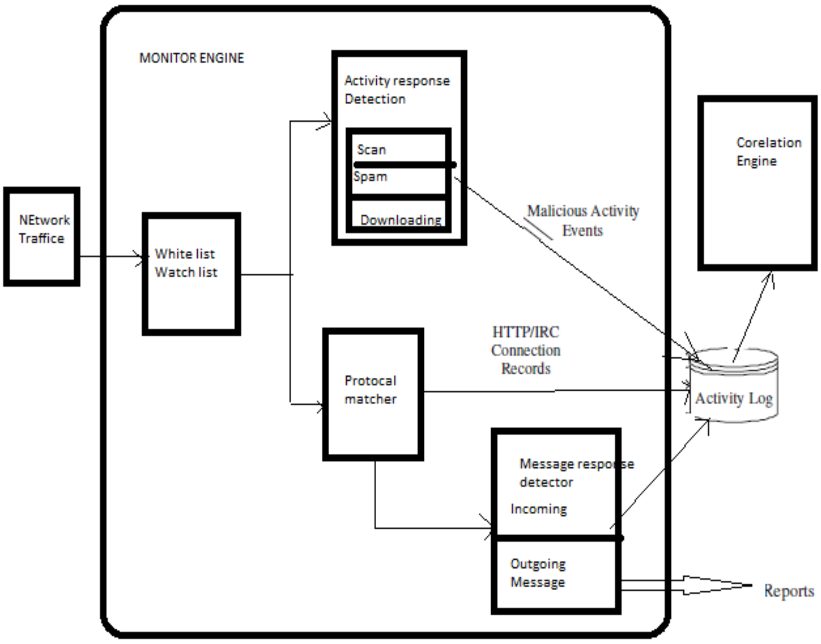

Figure 4: Bot Sniffer Architecture

In the result of this paper bots are detected very well with few false positive. Its correlation generates concise report rather than only producing the alert of the malicious events. This system to detect the intrusion in the virtual network is better than the existing systems. In the existing system if bots change their nick name then existing systems cannot detect these but as this system is only depends on the response so no any effect will take place iff nick name of the bots will change. Iff botnet sniffer is detect anomaly in very well but this methods fails in some case such as if some of anomaly use whitelist as a third party then it may be hard to detect bots in the botsniffer. In the proposed system encryption is not done but in the future work it will be possible to generate the encrypted communication content. In future author will try to improve the accuracy in the bot detection and resilience evasion and performing more and in real time environment.

6. Using uncleanliness to Predict Future Botnet Addresses

Now a days use of the botnets is increase rapidly to use as a malware tool. But this is to difficult to find out the future address of the botnets. This method is totally depends on the tracking the future address of the botnets. In this we have used one word that is ceaseless network. Botnets attack tool are very common due to the anonymity, flexibility provided by them to the attackers. In this we have some hypothesis that the attacker does not have knowledge about the target expect that target is vulnerable. If attacker not able to distinguish between host and other then he can attack on any one of them. In advance if attacker does not know to what host is vulnerable to then it can only attack on the host he have with him. If host is does the compromise with the attacker then attacker can do all spam, scan and denial of service attack on that host with other also. We have does the assumption that network is clean so that host cannot make any assumption about the host attack. This paper can give idea to predict the future host activity by analyzing the networks past activities. Here author have considers only hypothetical cleanness of the network. As this method totally depends on the spatial cleanness of the network. It will helpful to detect the future activity of the network but it will not work if the network is not cleanness.

7. Zombie Roundup: Understanding, Detecting, and Disrupting Botnets

Now a days on the internet all attack are happened in the schools and universities also. the commonly this attack is work by sitting on the home also this attack are also known as the bot attack or known as a zombie army or simply botnet. The botnets attacks are till now not well understand and studied. Authors have studied the how to detect the bot by directly monitoring the IRC or by monitoring the command and control channel. There is one new attack is coming now a days and affects the common people in their day to day life and also to the businessman. In this attack data is stolen and then it may be used for the make reputation down or to make a bad image of that person. The proposed method in this paper mainly focuses on the symptoms of these, checking the spam, also hardening the web browsing and detects the fishing attack as well. There are three main approaches to avoid the botnet one is the prevent the system from the infection and second one is the check the command and control among the hosts and host and the controller. Third one is the detect the secondary feature of bots. In the first approach we are using software such as firewall, antiviruses and some patching techniques. In the second method we are directly detect the botnets command and control traffic. In third approach we have use to make watch on the feature of the botnets instead of directly taking watch on the command and control channel. In this paper author focuses on the second and third approach of the avoiding the botnets. This paper only give the idea about the taking watch on the command and control line and another approach is make watch on the features of the botnets. This method only describes the detection of the botnets not to stop them. For example here they have used method like leave one gang member so that he can contact with other gang men and we will get all the information about the all the gang. This is the future work of this paper.

8. Modeling Botnet Propagation Using Time Zones

In this paper author described the use of time zone and location of the botnet to detect the attack. In this paper we are taking watch on the zombie handled by the attackers. In this paper author take data from the dozens of the botnet and billions of the victim of that attack. This approach will note down the area of propagation of the worm and in which time zone it will propagate. It will help to predict the next attack of the worm in the next time zone. In this malicious or victim computer are take under watch and the emails reach to the victim are first stored on the server before reaching to the victim computer machines. This model has some limitation such as if computer machine is switch off then system cannot get the time zone of the propagation of the warm. As compared to the existing system this system will helps to recognize the time zone of the worm as worms are continuously grown up. This model was more accurate than the SIR model currently used. The future work of this paper is to study the botnets in details so that further study the botnets that does not use the centralized C and C channel. This work has two primary keys one is the time zone of the botnet propagation and second one is the time of release. Author want to improve his research by doing mixed operating system, mixed applications and more things to study the botnets attack in details

9. Analysis of the Papers and NICE Method

As we have studied different types of the articles which have studied on the botnet attacks. Among them first paper address to the cloud computing environment and how cloud computing becoming the victim of the botnet attack. This will not give the idea about to avoid the botnet attack. In the second method that is in the bothunter method author proposed an evidence trail method to detect the botnet. In this need to keep watch on the sequence of the events occur during the command. Bothunter method is mainly depends on the preconditions and post conditions of the attack. Third one is the botsniffer method author have used control the command and control channel to avoid the botnet attacks. In the next paper author focused on the two methods to avoid the botnets. One is to make watch o the command and control channel and another one is to don’t directly watch the channel instead watch the feature of the botnets. As compared to all the studied methods we can conclude that nice method is very advanced than the other existing methods. In the proposed method we have proposed novel approach to detect and mitigate the intrusion in the virtual cloud environment. NICE uses the attack graph model to detect and prevent the attack in the cloud environment. The NICE also helps to introduce how to switch the programmable software model. The system performance evaluates the feasibility of the NICE. The proposed system surely minimizes the vulnerability in the cloud network and surely reduces the attack in the cloud environments. NICE only investigate the IDS to detect the zombies attack in the virtual cloud environment. In advance to the proposed system we are also studying to invent decentralized network control and attack analysis.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] M. Collins, T. Shimeall, S. Faber, J. Janies, R.Weaver, M. D. Shon, and J. Kadane. Using uncleanliness to predict future botnet addresses,. In Proceedings of the 2007 Internet Measurement Conference (IMC’07), 2007.

[6] E. Cooke, F. Jahanian, and D. McPherson. The zombie roundup: Understanding, detecting, and disrupting botnets. In Proceedings of Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI’05), 2005.

[7] 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.

[8] D. Dagon, C. Zou, and W. Lee. Modeling botnet propagation using timezones. In Proceedings of Network and Distributed Security Symposium (NDSS ’06), January 2006.

Author Profile

Ms. Rupali Pravin Adhau received B.E.(Computer Engineering) from North Maharashtra University. (2011).Currently she is pursuing M.E. in Computer Engineering from Institute of Knowledge College of Engineering, Pimple Jagtap, Pune, Maharashtra, India.

Prof. Saba Siraj is working as Assistant Professor **in** Institute of Knowledge of COE, Savitribai Phule Pune University, Pimple Jagtap, Pune, Maharashtra, India.