International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 19 (2015)

IEEE Sponsored 1st International Conference on Advanced Engineering and Technology for Sustainable Development (ICAETSD 2015)

Security enhancement in virtual networks and prevention of botnet intrusions using EIDS

Suganya.M
Department of Computer Science
Jansons Institute of Technology
Coimbatore,India.
madhisugi20691@yahoo.com

K..Moorthi
Department of Computer Science
Jansons Institute of Technology
Coimbatore ,India.
moorthicse@gmail.com

V.Sakthivel
Department of Computer Science
Jansons Institute of Technology
Coimbatore ,India.
mvsakthi@gmail.com

***Abstract*— Virtualization technologies have altered the concept of a network endpoint and appropriate endpoint security measures. Network security and auditing methods are extended to the physical machine level were considered to be satisfying. But, the virtualization has split the physical machine into virtualized servers and resources, creating the necessity of some modifications in the network security pattern. While traditional perimeter and internal security devices are not capable of addressing the fully virtualized environment resources and security risks. Virtual machines in the cloud are subjected to more vulnerabilities and attacks. These attacks can be induced in the cloud using botnets which is one kind of attacking scenario. All these attacks in any cloud environment makes it difficult for the network manager to prevent the virtual machines from the attacks. It is necessary for an Intrusion Detection System in a virtual domain to identify and reconfigure the network avoiding the intruders and attackers in a virtual environment. The Enhanced Intrusion Detection System (EIDS) deals with identifying those intrusions and it provides alerts to the virtual machines that are more prone to the attacks with a reduced false positive rate. The efficiency of EIDS has been validated in a virtual environment using the xen hypervisor which proves EIDS to be efficient in detecting the botnet intrusions.**

Index Terms—Security, Virtual network, Botnets, Intrusion, IDS.

I. INTRODUCTION

As virtual servers are moved to new environments, they have the capability of compromising the security of their new environment. Images that have been unused may not updated with current security measures. As with physical networks, virtualized networks need to ensure only authorized individuals and devices are allowed to access the network and communicate. Any unauthorized access need to be identified and restricted in an appropriate manner. As with physical networks, virtualized networks are vulnerable to intrusions that can lead to several interruptions and other consequences. In a physical network configuration, these interruptions can be verified by tracing physical connections which is not possible in case of virtual environments. In a virtualized environment, multiple virtual servers (virtual machines or VMs) share a common physical host machine. Generally the hosts and virtualized components require similar security precautions as that of any non-virtualized resource. The virtual environments have their unique security challenges that are not addressed by traditional security solutions.

Externally-based threats can be controlled with a virtualized security system deployed inside the virtual environment

Other intra-host threats include legitimate inter-VM communication and unauthorized access. These threats may transit virtualized LAN segments unseen by external security solutions or systems inside a virtual server. The resulting gaps create an unmonitored, unprotected security hole that may expose virtual machine to unauthorized access, infection, Denial of Service (DoS) and more [13].

The attackers follow several attacking scenarios to attack the virtual network. One of such scenario is the botnet, where one particular virtual machine acts as the attacker (Botmaster) and commands other virtual machines (Bots) in the virtual network to act as its slaves and make them to attack other machines connected to the cloud virtually. The Botmasters use C&C channel to communicate with the Bots.

All these attacks in any cloud environment makes it difficult for the network manager to prevent the virtual machines from the attacks. It is necessary for an Intrusion Detection System in a virtual domain to identify and reconfigure the network avoiding the intruders and attackers in a virtual environment.

In order to identify these attacks several Intrusion Detection System (IDS) has been proposed. Some of the IDS systems proves to be efficient but the false positive rates in detecting and reporting the intrusions are comparatively more.

The EIDS proposed in this paper detects the intrusions by generating the attack graphs, which gives the attack information including the information about those virtual machines that are having the possibility of getting attacked in future without any duplication hence reducing the false positive rates.

II. RELATED WORK

Udaya Tupakula, et al., with a unified security policy, the virtual domain groups the related virtual machines running on different physical machine into a single network domain. The virtual machines are capable of running different operating systems and applications, which makes it easy for the attacker to exploit any single vulnerability in any one of the VMs for attacking other machines in the virtual network. The IDS is to

be designed and developed considering the specific features of attacks, security policies.

As the availability of ways for intrusion occurrences in a virtual network is increasing more day-by-day, the intruders are becoming stronger and stronger. Jing Liu, et al., used the Botnet attack scenario for the study of intrusions. It describes the fundamentals of Botnets and related attacks, detection, tracing and countermeasures. The study includes the 4 stages in the lifecycle of Botnet. In every stage of its lifecycle, bots gain more access into the network.

Kassidy Clark, et al., [4] have explained the effect of bots in cloud environment. Many Cloud Service Providers (CSP) offer access to scalable, reliable computing resources following a pay as-you-go model. Research into security of the Cloud focusses mainly on protecting legitimate users of Cloud services from attacks by external, malicious users. Two experiments demonstrate the simplicity and low cost of launching such attacks. Porting traditional Botnet detection techniques to the Cloud is not straight forward, thus new techniques are required. One possible techniques extrusion detection. This would require CSPs to monitor outbound traffic to detect and respond to suspicious activity. Current policy is to wait until the victims of attacks contact the responsible CSP at which point action is taken to disable the attack. Until CPSs implement a comprehensive Botcloud detection and removal policy, Botmasters will continue to move their malicious activities into the Cloud and Botclouds will continue to grow.

There are several techniques proposed for intrusion detection in virtual machines described in [5] to [8]. Sheharbano Khattak, et al., [5] developed a community driven tool for botnet detection. This has two limitations which includes case specificity and rigidity. Jerome Francois, et al., proposed a technique called MapReduce which is a distributed computing framework using the PageRank algorithm. The experimental results are reported from an Hadoop cluster and the performance benefits are highlighted when using real network traces from an internet operator. G.Gu, et al., [7],[8] proposed BotHunter and BotSniffer where dialogue-based correlation, spatial-temporal correlation and similarity properties are utilized for bot identification respectively.

O. Sheyner, et al., [9] have modeled the network using graphs for easy understanding and analysis of the network. Attack graphs are manually produced by Red Teams. Construction by hand is tedious, error prone and impractical for attack graphs larger than a hundred nodes. In this paper, they have presented automated technique for generating attack graphs. This algorithm is implemented in a tool suite and tested over a small network with an intrusion detection system.

III. Enhanced Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of flavors and approach the goal of detecting suspicious traffic in different ways.

The word "Botnet" is derived from Robot and Network. They commonly use a C&C channel to send commands to their slaves. The C&C server can either be an IRC or HTTP server. The slaves are referred as bots which receive commands from the botmaster in two ways.If the server used is IRC then it is push style where the attacking system sends their orders to the bots. In the http server, the bots themselves periodically receive the commands. In both methods all the bots receive similar command simultaneously. This is one of the most threatening attack method followed by intruders to attack virtual networks.

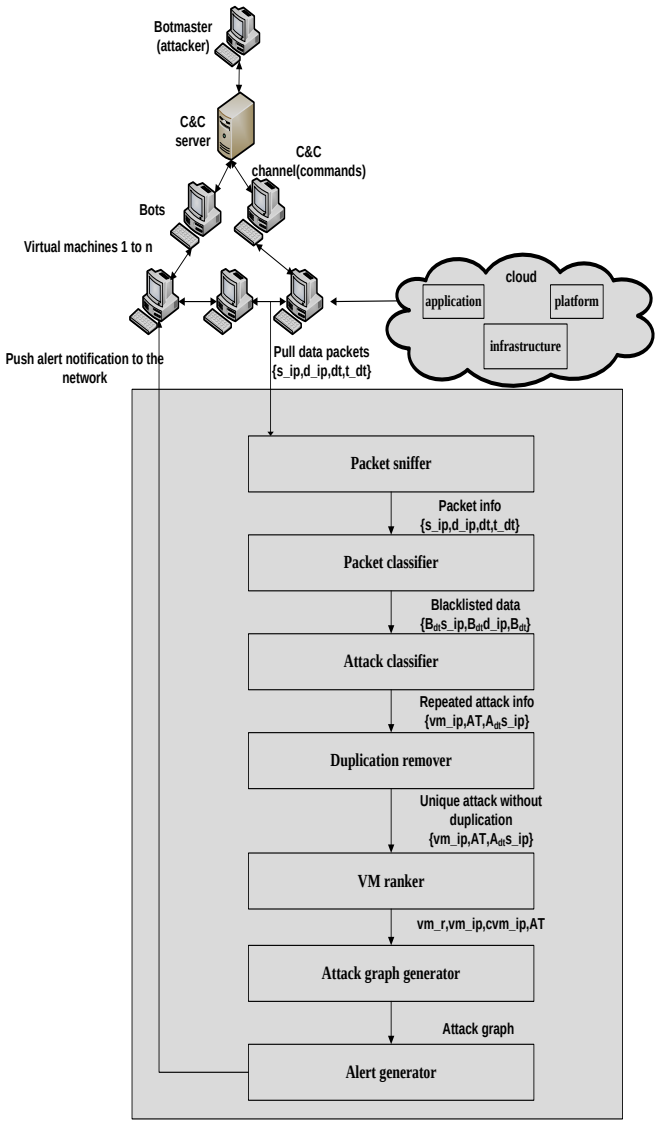

Fig. 1. Conceptual flow of EIDS with Botnet scenario

The conceptual flow of the EIDS architecture is depicted in figure 1. The packets along with the source and destination ip are sniffed from the network and stored in the databases. The packets are fetched from the database and on comparing the characteristic and activity of the data, they are classified in two

lists as Whitelist and blacklist. Blacklist is then collected from database and attack classification algorithm is applied to classify attack information and stored in the database.

The attacks have to be identified along with the attack information which includes source, destination, time and type of attack. Another module named duplication remover and VM ranker is used inorder to remove attack duplications for better performance of IDS avoiding the false positives.

A. Packet Sniffer and Classifier Algorithm

1. For each datapacket that flows in the network, collect the source ip(s_ip), destination ip(d_ip), time of arrival(t_dt).
2. Compare the source ip of the datapacket with that of the C&C server ip

If C&C_ip==s_ip, then

move the Dt, s_ip, d_ip & t_dt information of the verified packet to the blacklist.

B. Attack Classifier Algorithm

Attacks can be targeted in many ways. They can be invisible to a basic user. Some of the attacks includes . DDoS Attacks, Spamming, Sniffing, Click fraud and Identity Fraud.

1. Retrieve each data from blacklist and check for unauthorized webpage access and if found any is said to be DDoS, url attacks.
2. Any occurrence of voting from same ip is categorized as click fraud attack.
3. A mail notified as spam by the user is recorded as spam mail attack.

After these attack classification, intruder's ip can be blocked from the network. The information along with the type and frequency of attack is stored in the database.

C. VM Ranking and Duplication removal Algorithm

On analyzing the attack information there is a possibility of duplication due to the repeated attacks on the same virtual machines. This paves way for increased false positive rates in an Intrusion Detection System. Therefore this creates the need for the removal of the multiple entries of same virtual machine with the same kind of attacks from the database. This will help in reduction of false positive rates.

1. Get the attack information from the classified list,

If(A_i_id && d_i_ip's occurrence>1),then
remove multiple entries keeping a single data
Else make a new entry in database
Where, A_i_id - ith type of attack
D_i_ip - destination ip of ith attack

2. Assign rank 1 to the VM whose frequency is high. Similarly 2,3,..,etc., ranks are assigned to other VM's in ascending order.

D. Attack graph generation and alert notification Algorithm

It is not easy to understand or analyse a large network. Hencethe network can be modelled as graph where the nodesare used in representing the devices, VMs connected to the network and edges represent the links between network devices. These graphical representations along with the attack information is known to be the attack graphs.

After the ranking of VMs, the VM which is ranked with the minimum number is assumed to have the highest priority and this is the VM that has more vulnerability. Therefore the VMs that is connected directly with the highly affected VM is notified with the alert message specifying the information about the zombie virtual machine.

As the duplications are removed in previous step, the presenceof false positive rates in EIDS system can be reduced.

1. The VM with the rank 1 is the VM that makes first node of the attack graph.
2. Similarly for the VMs with rank 2,3,...,etc., as new nodes.
3. Any VM which forms as a new node in the attack graph having connected to a normal VM in the network, then the normal VM is given alert about the attacker.

This helps in identification of the attackers among many virtual machines connected to a common source.

IV. Performance Evaluation

The EIDS has been implemnented and tested in the hypervisor(xen), which is a virtualization tool that helps us in creating a virtual cloud like environment with a number of virtual machines connected to a common virtual server. One of the operating system acts as a Dom0 which is the host OS and other VMs are DomU (guest operating systems). Dom0 has a direct I/O path with the hypervisor whereas VMs in DomU has a virtual I/O path with to communicate with the xen server.

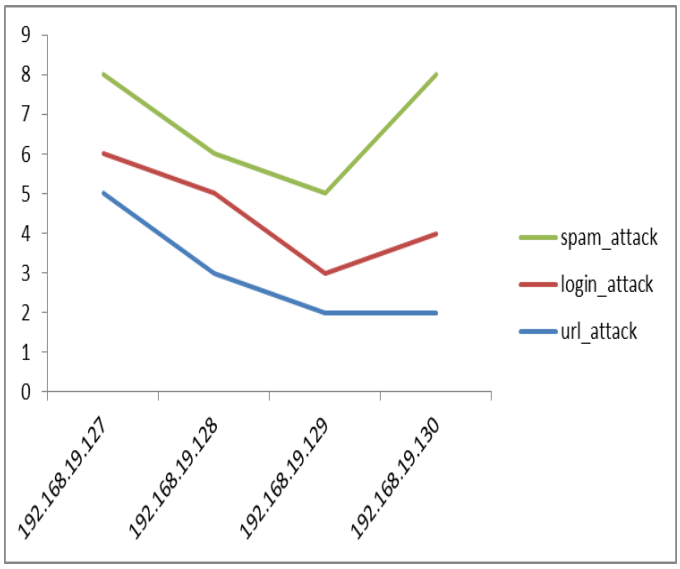

Fig. 2. Detected attack status in VMs

Also EIDS evaluation produce the report which shows the intense of attack in each virtual machine present in the network. This helps the admin or the network management team to analyze and reconfigure the network based on the intensity of attacks in virtual machines.

V. CONCLUSION

As the vulnerabilities in the virtual environments are increasing day by day, it drags the attention of the security providers to prevent those attacks and identify the vulnerabilities. This Enhanced Intrusion Detection System (IDS) sniffs the packets from the network and classify the packets accordingly and alerts the normal virtual machines to be aware of the zombie machines. The previous Intrusion Detection Systems produce increasingly more false positive rates in detecting the attacks in virtual domains, hence this system helps in avoiding those false positives by removing the duplications in the attack and provides notification to the normal virtual machines on the attack scenario and protects those virtual machines from such kind of vulnerabilities. The work can be extended by detecting the intrusions also by considering the characteristics of the virtual machines as they vary in different aspects based on their requirement in the virtual domain system. As the intruders are becoming strong new attacking scenarios are arising which creates the need to detect any such new attacks dynamically by the intrusion detection systems.

REFERENCES

[1] Udaya Tupakula, Vijay Varadharajan, and DipankarDutta, "Intrusion Detection Techniques for Virtual Domains," Proc. IEEE 2012.

[2] Chun-Jen Chung, PankajKhatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[3] Jing Liu, Yang Xiao, KaveshGhaboosi, Hongmei Deng, and Jingyuan Zhang "Botnet:Classification,Attacks,Detection,Tracing, And Preventive Measures," EURASIP Journal on Wireless Communications and Networking, Volume 2009, doi:10.1155/2009/692654.

[4] Kassidy Clark, MartijnWarnier, Frances M.T.Brazier, "BOTCLOUDS- The Future of Cloud-based Botnets?," Proc. Techno-Pulse Nov 2010.

[5] SheharbanoKhattak, Zaafar Ahmed, Affan Syed, Syed Ali Khayam, "BotFlex: A Community-driven Tool for Botnet Detection," CCS'13 Nov 04-08 2013, Berlin, Germany ACM 978-1-4503-2477-9/13/11.

[6] Jerome Francois, Shaonan Wang, Walter Bronzi, Radu State, Thomas Engel, "BotCloud:Detecting Botnets Using MapReduce," Proc.IEEE 2010.

[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), pp. 12:1-12:16, Aug. 2007.

[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.

[10] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling. The nepenthes platform: "An efficient approachto collect malware". In Proceedings of Recent Advances in Intrusion Detection, Hamburg, September2006.

[11] Benoit Jacob, "Experimental Host and Network-based Analyser and Detector for Botnets".Computer Networks and Distributed Systems in School of Computing, April 2010.