INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 5 ISSUE 4 (2019) PAGES 4436 - 4438
RECEIVED : 12.06.2019 PUBLISHED : 16.07.2019

July 16.2019

# EFFECTIVE DETECTION OF THE DYNAMIC ATTACK PATTERN FROM LOGS ANALYSIS FOR VIRTUAL MACHINES IN CLOUD

[1]Anupriya. R , M.Phil, Research Scholar, K.M.G College Of Arts & Science, Gudiyattam.

[2]Prof.P.Anjugam, Assistant Professor, Pg & Research Department Of Computer Science & Applications

**Abstract**:

The continuously emerging, operationally and managerially independent, geographically distributed computer networks deployable in an evolutionarily manner have created greater challenges in securing them. Several research works and experiments have convinced the security expert that Network Intrusion Detection Systems (NIDS) or Network Intrusion Prevention Systems (NIPS) alone are not capable of securing the Computer Networks from internal and external threats completely. In this paper we present the design of Intrusion Collaborative System which is a combination of NIDS,NIPS, Honeypots, software tools like nmap, iptables etc. Our Design is tested against existing attacks based on Snort Rules and several customized DDOS , remote and guest attacks. Dynamic rules are generated during every unusual behavior that helps Intrusion Collaborative System to continuously learn about new attacks. Also a formal approach to deploy Live Intrusion Collaboration Systems based on System of Systems Concept is Proposed.

**Keywords**: Network Intrusion Detection, Network Intrusion Prevention, IPTABLES, Honeypot and NICS.

## 1. INTRODUCTION

A Comparative Study of Network Intrusion in Detection Systems in[1], In 2008 Moses Garuba, Chunmei Liu, and Duane Frates have conducted an extensive study on the different Intrusion techniques [1] and they also demonstrated that NIDS alone cannot handle both internal and external threats to computers. They also proposed that Heuristic Based solutions are better than signature based solutions. Self Adaptivity and Dynamic analysis are the key features that have to be there in any NIDS as the responsiveness for any NIDS is determined by these properties. In [2] the importance of dynamic behavior of the NIDS is demonstrated by Zang Qing Hua , Fu Yu Zhen, Xu Bu-gong . Luis Carlos Caruso and others have submitted their proof of concept on huge computing power requirement for signature based NIDS called SPP-NIDS [3]. The limitations as mentioned In [4] and [5] after a certain communication link speed NIDS will fail to perform as the load increases and softwares like SNORT [4] require a huge computing capability to handle communication line greater then 100Mbps. Miyuki Hanaoka and others have discussed the importance of collaboration between the security mechanisms and They also demonstrated that redundant rules could be eliminated between the NIDS with a collaborative model. NIDS alone is not sufficient to handle entire range of threats and attacks on the computer networks. Network Intrusion Preventive mechanisms will also help significantly in reducing the effect of an attack over a computer network. Network Intrusion Preventive mechanisms like traditional firewall along with strong authenticating procedures in collaboration with NIDS will make a computer network more secured Firewall play a vital role in NIPS, Despite taking all these precautions attacks still happen and the computer security system still fails to secure the computer networks in case of new type of attacks. Hence a mechanism where it would be possible for the attackers to get trapped unknowingly so that the systems can secure the computer networks from getting infected is essential. HoneyPots [9] can be used to secure the computer network along with NIDS and NIPS. Honeyd is a small daemon that creates virtual hosts on a network.

 

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 5 ISSUE 4 (2019) PAGES 4436 - 4438
RECEIVED : 12.06.2019 PUBLISHED : 16.07.2019
July 16.2019

## 2. RELATED WORK

Though the security system is setup in each network it is very important to deploy the mechanisms at proper places. It is important the reporting mechanism is highly reliable as the centralized server will be taking the report from the sub systems. Section 2 describes the procedure of setting up and deployment of Network Intrusion Collaboration System. Section3 describes a formal approach of Systems-of-Systems towards effective deployment of Intrusion Collaborative system in a distributed manner. Administrator will decide on blacklisting IP in case of any attacks , threats or anomalous behavior based on the information obtained from attack classifier. NIDS was also deployed at appropriate locations to check the internal attacks in every subnetwork. The information about the activity of the subnetwork within the network was always collected and sent to the central server to take corrective measures to avoid threats from internal resources. An aggregate DDOS attack pattern generator.

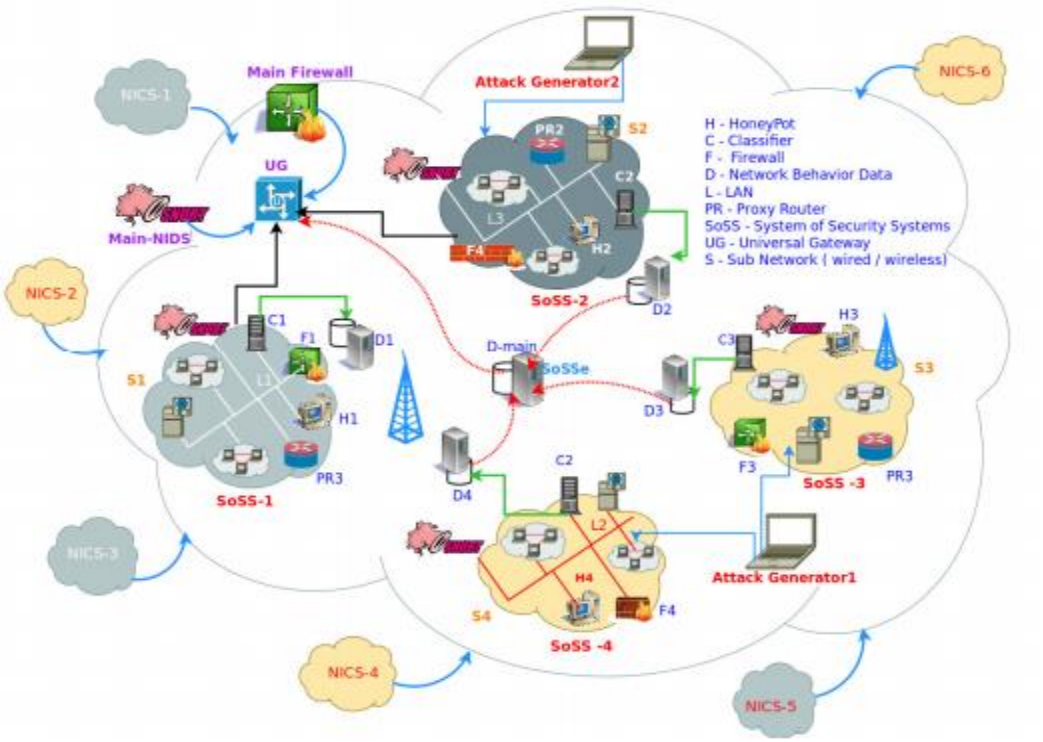


**Fig.1. Setup Structure**

These System of Security Systems(SoSS) in each subnetwork must collaboratively work together to fight against intrusions. SoSS will eventually become Operationally independent of one another, Managerially independent of each System, Deployable in an Evolutionary manner, Emergent, Distributed Geographically, and Heterogeneous while Networking with Systems.

## 3. ANALYSIS

With the introduction of the NIDS, Firewall, Classifier and Honeypot in each SOSS , The security level of each subnetwork is increased by 50 %. Also the efforts in tracing the abnormal activities is minimized exponentially since most of the traffic filtering can be done at the firewall and NIDS. In Subnetwork firewall and NIDS takes care of detecting major known anomalous behavior using signatures and concentration will be on the new type of attacks which will be easily traced with the honeypot and reported to the classifier and again reported to the main server to record the abnormal activity to take corrective measures by the

 

administrator. This mechanism also reduced the number of alarms usually raised by the NIDS upto 70%. Honeypots and NIDS detect the abnormal behavior during an internal and external DDOS attack within 5 seconds and were able to take corrective measures within 7 seconds whereas a network without Honeypot was clogged within 12 seconds and the switches were completely non functional and entire system was supposed to be shut down. With the introduction of the firewall and a proxy router at each subnetwork , traffic filtering task was simplified. Universal Gateway had the major responsibility of deciding the genuineness of an activity. Always it is possible to sneak into the network but the intruder or attacker will always look for the compromised system and Honeypots will be able to easily trap them and report their interactions to the classifier to dynamically either blacklist those machines or prevent them from doing further damage.

## CONCLUSION

A Honeypot based Network Intrusion Collaboration System which is capable of generating dynamic rules during any anomalous behavior in the network or a possible intrusion is presented. The NICS designed is a collection of several existing Free and Open Source Softwares customized for the specific need that helps in implementing both preventive and detective mechanisms of network security. Honeypot based NICS was capable of identifying the customized intrusion and other abnormalities in the traffic over network which were generated during attacks faster than conventional methods.

## REFERENCES

[1] Moses Garuba, Chunmei Liu, and Duane Fraites (2008) “Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems ” Fifth International Conference on Information Technology: New Generations , Page 593-598, DOI 10.1109/ITNG.2008.231
[2] Zang Qing Hua , Fu Yu Zhen, Xu Bu-gong (2008),” A New Model of Self Adaptive Network Intrusion Detection System” , 978-1-4244-1823-7/08, Page 436-440
[3] Luis Carlos Caruso, Guilherme Guindani, Hugo Schmitt,Ney Calazans, Fernado Moraes, 2007 SPP-NIDS-A Sea of Processor Platform for Network Intrusion Detection, 18th IEE International Workshop on Rapid System Prototyping,
[4] http://www.snort.org [5] Miyuki Hanaoka, Kenji Kono, and Toshio Hirotsu, 2009, “Performance Improvement by means of Collaboration between Network Intrusion Detection Systems”,2009 Seventh Annual Communications Networks and Services Research Conference, DOI 10.1109/CNSR.2009.48, page 262-269
[6] Simon P. Chung and Aloysius K., Mok phchung, mok , 2005, Collaborative Intrusion Prevention, N00014-03-1-0705