International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Zombie Attack Analyser and Counter Measure In Cloud

Lokesh A. Kochekar[1], S. P. Washimkar[2]

[1, 2]Department of Electronics and Telecommunication, Priyadarshini College of Engineering, Nagpur, India

Abstract: ***Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this field has focused primarily on denial of communication at the routing or medium access control levels. Exploring resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Zombie" attacks are not specific to any specific protocol, but rather rely on the properties' of many popular classes of routing protocols. We find that all examined protocols are susceptible to Zombie attacks are very and difficult to detect and are easy to carry out with the normal data. A single zombie attack increases the data size. We discuss the methods to detect and stop this kind of attack. For this We create a network showing how the data is transfer from source to destination and also monitors whether the given data is normal or the data is infected by zombie attack.***

Keyword: network nodes, malicious conditions

1. Introduction

Virtual machine is supposed to be consider as the safety risk in cloud system because of the fact that all user that uses cloud set up their applications in virtual machines. specially , intruders can damage their vulnerability to a cloud system and nagotiate virtual machines to deploy large scale types of attack like distributed denial of service (DDOS). Particularly when susceptibility produce in infrastructure as a service cloud where the infrastructure were shared by millions of users. We want to protect vulnerable virtual machine from being negotiated in the cloud , the proposed framework introduces multiphase distributed vulnerability detection measurement and countermeasure selection mechanism. It will creates an attack graph analytical model which is useful for detecting the intruders possible way of exploit vulnerability. The model consist of information related with topology i.e virtual and also information about cloud servers. Based on that information given by the analytical model then the system gives an appropriate counter measures.

2. Problem Definition

Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. Specially attackers can explore vulnerabilities of a cloud system identified vulnerable virtual machines as zombies attacks. It is Clustering-based Classifier Selection Method for Zombie attack detection and its counter measure.In this paper we studied the pattern recognition approach based on classifier selection to network zombie attack detection and proposes a clustering-based classifier selection method.

Tal Garfinkel Mendel Rosenblum
A Virtual Machine Introspection Based Architecture for Intrusion Detection.In this we studied an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. Approach for intrusion detection which co-locates an IDS on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate the IDS from the monitored host.

3. Literature Survey

ISSN: 2278-0661 Volume 3, Issue 1,
Dr.Balachandra, D.N.Karthek
(July-Aug. 2012)

An Overview on Security Issues in Cloud Computing In this paper we have studied how security and compliance integrity can be maintained in new environment the prosperity in Cloud Computing literature is to be coming after security and privacy issues are resolved.

Vol.3, No.4, Hamoud Alshammari and Christian Bach, August 2013 Administration Security Issues In Cloud Computing In this paper we have studied most administration security issues and concept of the Service Level Agreement or any trust third party that can control the processing over Could Computing The solution to get more secure Cloud Computing environment is to have a strong Service Level Agreement Offering an adequate level of security and privacy for the information that is already in the cloud.
ISSN: 2305-0012,Sina Manavi, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah,2012 Secure Model for Virtualization Layer in Cloud Infrastructure In this paper we have studied to propose a model to secure and proper mechanism to react reasonable against the detected attack by intrusion detection system. With the secured model (SVM) against the attack SVL model, (Secure Model for Virtualization layer)which combines virtualization and intrusion detection system, can increase the detection rate and provide protection against attacks targeting virtualization, and consequently will result in reliable cloud security the proposed model and framework will be implemented in order to compare and evaluate it with the traditional manner .

ISSN : 2248-9622, Vol. 4, Issue 3(Version 5) ,Mr. V.V.Prathap, Mrs.D.Saveetha,2014 Detecting Malware Intrusion in Network Environment In this is model we have studied three model intrusion detection Threat model,Attack Graphe model,Existing model NICE utilizes the attack graph

model to conduct attack detection and prediction. NICE only investigates the network IDS approach to counter zombie explorative attacks.

VOL. 10, NO. 4 Chun-Jen Chung,Tianyi Xing,Dijiang Huang,2013 NICE: Network Intrusion Detectin and Countermeasure Selectionin Virtual Network Systems In this paper we have studied The system and security evaluations demonstrate the efficiency and effectivenes of the proposed solution NICE, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE only investigates the network IDS approach to counter zombie explorative attacks. To improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system.

Shina Sheen,R Rajesh Network Intrusion Detection using Feature Selection and Decision tree classifier. In this paper we have studied three different approaches for feature selection, Chi square, Information Gain and ReliefF which is based on filter approach Intrusion Detection with feature selection was able tooutperform the decision tree algorithm without feature selection Intrusion Detection approach is very useful for counter measure ijceronline.com) Vol. 2 Issue. 7 ,Prof.D.P.Gaikwad , Pooja Pabshettiwar, Priyanka Musale,Pooja Paranjape,Ashwini S. Pawar,2012 A Proposal for Implementation of Signature Based Intrusion Detection System Using Multithreading Technique

In this paper we have studied signature based intrusion detection system, using multithreading technique. The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. multithreaded technique for better intrusion detection should be distributed and cooperative by applying co-operative agents to the network.

Vol.5, No.2, Shalvi Dave, Bhushan Trivedi and Jimit Mahadevia, 2013 Efficacy of attack detection capability of IDPS based on its deployment in wired and Wireless environment. IDS logging agent inspects the data with the help of Suricata. Suricata is an open-source IDS available on all the platforms. It identifies an attack based on pre-defined signature rule-set.
Intrusion Detection and/or Prevention Systems (IDPS) represent an important line of defence against a variety of attacks that can compromise the security.

IEEE 12th International Conference on Data Mining Workshops, Anand Kannan and Gerald Q. Maguire,Ayush Sharma and Peter Schoo,2012 Genetic Algorithm based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Networks In this paper we have studied a new intrusion detection model in which we combine a newly proposed genetic based feature selection algorithm and an existing Fuzzy Support Vector Machines (SVM) for effective classification as a solution. New genetic based feature selection algorithm is used to select optimal number of features from the KDD cup data set for intrusion detection.

Genetic algorithm is very helpful for intrusion detection.

978-1-4244-6005-2/10/$26.00 ©IEEE ,Aizhong Mi Linpeng Hai,2010.
A Clustering-based Classifier Selection Method for Network Intrusion Detection.

In this paper we studied the pattern recognition approach based on classifier selection to network intrusion detection and proposes a clustering-based classifier selection method.

The pattern recognition technique to intrusion detection, and proposes a network intrusion detection approach based on multiple classifier selection, called CDS. This method is very useful intrusion detection

Tal Garfinkel Mendel Rosenblum
A Virtual Machine Introspection Based Architecture for Intrusion Detection.
In this we studied an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. The pattern recognition technique to intrusion detection, and proposes a network intrusion detection approach based on multiple classifier selection, called CDS. This method is very useful intrusion detection.

Tal Garfinkel Mendel Rosenblum
A Virtual Machine Introspection Based Architecture for Intrusion Detection.
In this we studied an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. Approach for intrusion detection which co-locates an IDS on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate the IDS from the monitored host.

4. Research Methodology

In this report, we propose Zombie attack detection and its counter measure which detects zombie attack and also stop it. For better attack detection this project incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design Zombie attack does not intend to improve any of the existing intrusion detection algorithms; indeed, Zombie creates a reconfigurable virtual networking approach to detect and counter the Zombie attack.

5. Design Module

User Module
We create a windows which show the network by sing c# language in dot.net. After that we show how the data is flow from soure to destination. Than we create a zombie attack and show its behaviour and than we do its counter measure to stop the zombie attack. Steps are to create a network ,than path is created to show how the data is travel after that we create a routin table and also create a encryption and decryption key for key management and security using MD5 and 3DES algorithm.

Countermeasure Selection
To detect zombie attack we create its counter measure which actually stops the attack and save the power consumption of the machine.

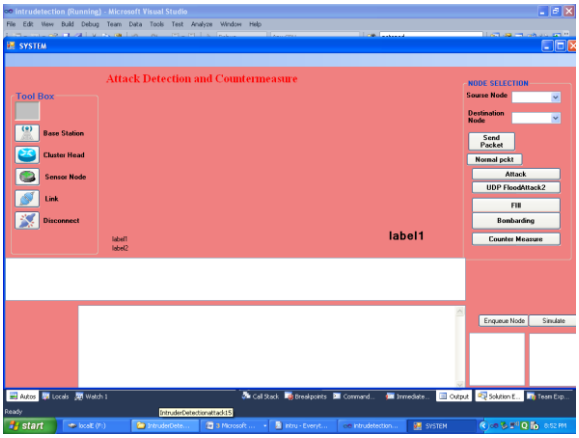
Attack Anylyser

The system has level of security for protection of data which verifies the packet for detection of intruder so that the countermeasure can be applied attacks usually involve early stage actions such as multistep exploitation, vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the system, especially the detection of zombie exploration attacks is extremely difficult. Another important function of the network controller is to assist the attack analyzer module. According to the controller receives the first packet of a flow, it holds the packet and checks the flow for complying traffic policies. The methods for selecting the countermeasures for a given attack scenario. When vulnerabilities are discovered or some are identified as suspicious, several countermeasures can be taken to restrict attackers' capabilities and it is important to differentiate between compromised and suspicious packets.

The countermeasure serves the purpose of: 1) protecting the target VMs from being compromised, and 2) making attack behavior stand prominent so that the attackers'actions can be identified. The proposed system is useful for any kind of network because verification methodology is implemented at each hop through which attack accuracy is improved. Attack is countermeasure before attack happened in network. The proposed solution is implemented in Network intrusion Detection System and Host-based Intrusion Detection which also improved the attack detection accuracy. Network traffic is not disturbed because attack completely countermeasure. Data is secured after attack happened because it prevented before its reaction. Countermeasure selection is useful after attack happened because with used of it network traffic is not disturb.

Valid Packet, Packet Generation and Packet Sent Successfully

We are assuming 64 bit data packet with 56 bit key for encryption and decryption. For this we are using 3DES and MD5 method available in dot net environment. Packet depends on its types and on the protocol. Normally, a packet has a header and a payload. The header keeps overhead information about the packet, the service and other transmission related things. Such as data packet structure, structure include source IP address, destination IP address, sequence number of packet, type of service, flags etc. The payload is the data it carries A cloud system with hundreds of nodes will have huge amount of alerts raised by Snort. Not all of these alerts can be relied upon, and an effective mechanism is needed to verify if such alerts need to be addressed. Since Snort can be programmed to generate alerts.



6. Conclusion

Thus the creation of normal data and the data containing zombie attack ius completed. Its counter measure is also completed. Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

References

[1] B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.

[2] H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[3] "Open vSwitch Project," http://openvswitch.org, May 2012.

[4] 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.

[5] 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.

[6] 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.

[7] 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,

[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] "NuSMV: A New Symbolic Model Checker," http://afrodite.itc. it:1024/nusmv. Aug. 2012.
[11] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graphbased network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS '02), pp. 217-224, 2002.
[12] X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic- Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005.
[13] R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Framework and Techniques," Proc. ACM Int'l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06), pp. 37:1-37:10, 2006.
[14] L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts," Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.
[15] S. Roschke, F. Cheng, and C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph," Proc. Fourth Int'l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.
[16] 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.
[17] 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.