ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (365-368), Month: April-June 2014, Available at: www.researchpublish.com

Security of IDS in Cloud Environment

Pooja[1], Shikha Pandit[2]

[1,2]Department of CSE, Maharishi Dayanand University
Palwal, INDIA

Abstract: **IDS in cloud environment is applied since years but its working is not yet proved. These days cloud computing is uses on the vast scale for accessing computing resources ,as in LAN use of IDS is not considered significant, due to limited users of LAN cloud environment is more in demand. In this research work, a cloud environment is tried to propose for IDS services in a limited manner or as per user's requirement. By using SNORT IDS software on virtual machine, we are executing this setup. With the help of WINSCP, we are fetching data from VM to windows or another system.**

Keywords: **IDS, CIDS, VMWare, WINSCP, LINUX software, PHP**

I. INTRODUCTION

In this research work, we are trying to execute a setup for cloud environment on virtual basis for limited use of services for limited users.

A. What is IDS

IDS is intrusion detection system, used to detect data packets or monitor a network.IDS comes in various approaches like detecting suspicious traffic on network .Some systems may cause stoppage to find an intrusion but no one can interrupt any intrusion.IDS generally record information regarding events, provide security alarms, notify bugs to the admin and produce reports .They use several response techniques which involves configuration of firewall ,attack counter ,modify security environment and security infrastructure.

Types of IDS:

IDS basically have three types. HIDS (Host-based IDS), NIDS(Network-based ISD) and DIDS. All these types are based on attack detection rate and prevention from intrusions. HIDS is used for host-based intrusion detection system, NIDS used for network-based intrusion detection system, DIDS used for distributed -based intrusion detection system. Other types of IDS can be said as behavior-based IDS, knowledge-based IDS.

B. What is cloud computing

1. Definition of cloud computing

Cloud computing is a paradigm analogous to Internet, which is based on cloud drawing. In earlier days, these clouds are used to show telephone networks. But now-a-days, its use is increasing vastly in computer technology. In internet, it is used to provide various services mainly, to deliver data packets over the Internet. It consists of a VMware which is responsible for providing all the services to cloud users. These services includes-providing software, application type, various devices, platform where to be used, its infrastructure and also provides hosting services to customer on pay-you-use basis .to use a cloud application and to access it, only a good browser and a suitable internet connection is required.

2. Benefits of cloud computing

1. No need to buy the full infrastructure, just buy the resources that you needed.
2. On cloud systems, large amount of data can be stored as compared to personal systems.
3. It updates the software automatically, cloud users need not have to bother about the enhancements or changes in its maintenance, hardware or software.
4. To access the data, no need to be sit on the desk. Anyone can use the data from any location.
5. Updates can be easily done to the clod system.
6. Its maintenance cost is less as compared to private systems.
7. Using cloud systems, data can be accessed in fast speed as compared to private systems.

II. IDS IN CLOUD ENVIRONMENT SERVICES

A. IaaS(Infrastructure as a service): IaaS is a model that provides various services to its cloud user. It includes services like providing hosting services to customer, routing services, and storage services by maintaining its vast infrastructure. With IaaS, an IDS can perform computing and billing services for purpose of dynamic scaling and desktop virtualization .IaaS a separate environment for how a VM uploaded on that environment and hosted it .IaaS is fully customer services that is used to differentiate various security signatures on different scenarios like user and admin.

B. PaaS(Platform as a service): PaaS model provides facility to a user to run and develop applications the desired platform. With PaaS model, network can perform hosting services, developing services and running services. Very serious DOS attacks and cloud service providers are controlled by PaaS platform. The major part of PaaS is to provide security so that cloud and grid can work simultaneously by achieving behaviors.

C. SaaS(Software as a service)**:** SaaS model delivers installation processes and execution of services on desired own machines. Presently DOS attacks and distributed DOs attacks can be handled by SaaS only. It is suited for all IDSs like HIDS, NIDS, and DIDS.

III. HOW CLOUD WORKS IN IDS

Cloud computing system's main goal is to provide security in distributed environment while delivering data packets over Internet. Cloud system consists of cloud users, suitable Internet connection and other devices(control node).it provides storage, maintenance services to the cloud users and provide services to administrators too. In the system, firstly cloud user sends the required request's to the cloud system via Internet. Then the request reached to a control node which is responsible for performing other services in the cloud. It monitors the request send by cloud user and analyzes it and makes a report on the information it gains after analyzing the request. To maintain a report it uses a help of its database servers. And finally sends the request to intended user in the cloud.

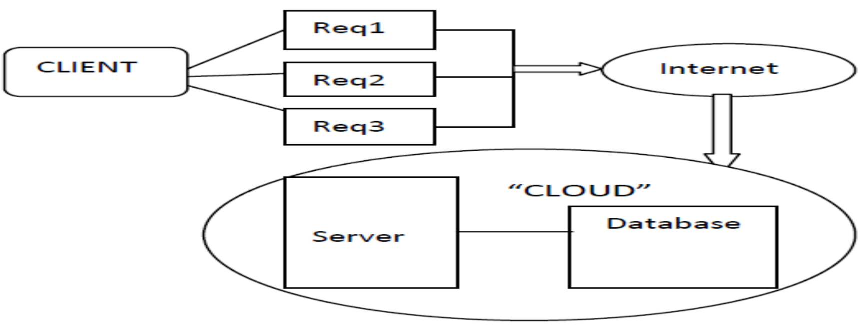

Figure1: How Cloud computing works

IV. PROPOSED WORK

Our model is an effective and efficient cloud IDS which uses IaaS services to improve CIDS performance over cloud network. Our multi-system environment will monitor network traffic as well as detected packets. Due to its implementation for cloud, the system sends instant report to cloud user organization and management system. With the rapid flow of huge amount of data moving in cloud environment, our VMware can be crashed due to large volume overloading. Only a network based CIDS can survive in such situation.IDS software will be applied on network points, routers or network monitoring tools. Nor the IDS not the users will monitor data packets, only a third party system or advisory part can see the monitoring services.

A. Advantages of proposed model:

If we compare the result of our proposed model with traditional IDS system, we find a lot of advantages over previous models.

1. Due to limited users, its saves manpower cost
2. Due to use of virtual cloud environment ,it saves hardware cost
3. It saves our system from data loss on high speed network/low speed network
4. Large volume of data will be serviced by different users, so no any user gets burden of data packets.
5. Memory efficiency is also a good part of this proposed model

V. CONCLUSIONS

In cloud computing, volume of data makes IDS administrator unable to analyze ,add ,delete, authorise, unauthorise, password security to monitor each user's activity. On the basis of readings comes as outcome of this proposed work will show an improvisation in on-demand services and detections. This model presents future architecture of IDS in cloud environment. A new fault-tolerant system is designed to make sure users reliability and elasticity of IP addresses. Using a number of controls can be ineffective and inefficient in LAN scenario, so this model is worked on cloud scenario.

VI. FUTURE WORK

In future work, this setup can be worked for large organizations and more security services can be applied in it .Later on, progress work for cost cutting and detection can be work for prevention of data in cloud environment. A global approach can be shared among industries and academic institutions for privacy for their data and information. We can also draw more refined results in form of graphs and tables .

ACKNOWLEDGMENT

I would like to say thanks all who helped me in successful creation of this paper. I would like to express my gratitude to Ms Shikha Pandit (Department of Computer Science and Engineering) as a guide who gives me full support and positive feedback during the preparation of this paper. Last but not the least, I am thankful to my friends and all other staff members whose suggestion helped me a lot to complete this paper.

REFERENCES

[1] Unspam; LLC a Chicago-based anti-spam company. “Website for the project honeypot,”. http://www.projecthoneypot.org/.

[2] M. Analoui, A. Mirzaei, and P. Kabiri, “Intrusion detection using multivariate analysis of variance algorithm,” in Third International Conference on Systems, Signals & Devices SSD05, vol. 3, Sousse,Tunisia, Mar. 2005. IEEE.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (365-368), Month: April-June 2014, Available at: www.researchpublish.com

[3] A. Zhong and C. F. Jia, “Study on the applications of hidden markov models to computer intrusion detection,” in Proceedings of Fifth World Congress on Intelligent Control and Automation WCICA, vol. 5, pp. 4352–4356. IEEE, June 2004.

[4] D. Barbara, J. Couto, S. Jajodia, and N. Wu, “Special section on data mining for intrusion detection and threat analysis: Adam: a testbed for exploring the use of data mining in intrusion detection,” ACMSIGMOD Record, vol. 30, pp. 15–24, Dec. 2001.

[5] D. Barbara, N. Wu, and S. Jajodia, “Detecting novel network intrusions using bayes estimators,” in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr.2001.

[6] M. Bilodeau and D. Brenner, Theory of multivariate statistics. Springer - Verlag : New York, 1999.Electronic edition at ebrary, Inc.

[7] M. Botha and R. von Solms, “Utilising fuzzy logic and trend analysis for effective intrusion detection,”Computers & Security, vol. 22, no. 5, pp. 423–434,2003.

[8] Susan M. Bridges and M. Vaughn Rayford, “Fuzzy data mining and genetic algorithms applied to intrusion detection,” in Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct.2000.

[9] D. Bulatovic and D. Velasevic, “A distributed intrusion detection system based on bayesian alarm networks,” Lecture Notes in Computer Science (Secure Networking CQRE (Secure) 1999), vol. 1740, pp. 219–228, 1999.

[10] J. Cabrera, L. Lewis, X. Qin, W. Lee, R. Prasanth, B. Ravichandran, and R. Mehra, “Proactive detection of distributed denial of service attacks using mib traffic variables - a feasibility study,” in Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management, pp. 609–622, Seattle, WA, May 2001.

[11] Joao B. D. Cabrera, L. Lewis, X. Qin, W. Lee, and Raman K.Mehra, “Proactive intrusion detection and distributed denial of service attacksa case study in security management,” Journal of Network and Sys- tems Management, vol. 10, pp. 225–254, 2002.

[12] S. B. Cho, “Incorporating soft computing techniques into a probabilistic intrusion detection system,” IEEE TRANSACTIONS ON SYSTEMS, MAN,AND CYBERNETICSPART C: APPLICATIONS AND REVIEWS, vol. 32, pp. 154–160, May 2002.

[13] NETSEC-Network Security Software Co. “Specter,”. http://www.specter.com/.

[14] NFR Co. “Website of nfr co.,”. http://www.nfr.net/.