A Hierarchical Intrusion Detection System for Clouds: Design and Evaluation

Hisham A. Kholidy [1,2,3]
hkholidy@ece.arizona.edu,
hisham_dev@yahoo.com

Fabrizio Baiardi [2]
baiardi@di.unipi.it

Salim Hariri [1]
hariri@ece.arizona.edu

Esraa M. Elhariri [1,3]
esraaelhariri@email.arizona.edu

Ahmed M. Yousof [1]
amyousof@email.arizona.edu

Sahar A. Shehata [1]
saharabdelfattah@email.arizona.edu

[1] NSF Cloud and Autonomic Computing Center, College of Electrical and Computer Engineering,
University of Arizona, USA.
[2] Dipartimento di Informatica, Università di Pisa, Pisa, Italy
[3] Faculty of Computers and Information, Fayoum University, Fayoum, Egypt

Abstract

Security and availability are critical for cloud environments because their massive amount of resources simplifies several attacks to cloud services. This paper introduces a distributed deployment and a centralized one for our Cloud intrusion detection framework, CIDS-VERT. After describing the architectures and the components of the two deployments it describes the experimental results that confirm that the deployments overcome some limitation of current IDSs to detect host, network and DDoS attacks. Lastly, we discuss the integration and the correlation of the host and network IDSs alerts to build a summarized attack report.

Keywords: *Cloud Computing, Security, Intrusion Detection, Attacks, DDoS.*

Published In: International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.6, December 2012, DOI: 10.5121/ijccsa.2012.2601

References

[1] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, "Detecting Masquerades in Clouds through System calls and NetFlow Data Analysis", Ready for submission to the IEEE Transactions on Dependable and Secure Computing Journal.

[2] http://technet.microsoft.com/en-us/library/cc959354.aspx

[3] http:/en.wikipedia.org/wiki/Attack_(computing)

[4] http://www.metasploit.com/

[5] Stein, Lincoln. The World Wide Web Security FAQ, Version 3.1.2, February 4, 2002. http://www.s3.org/security/faq/ - visited on October 1, 2002.

[6] Zaroo, P.; "A survey of DDoS attacks and some DDoS defense mechanisms", Advanced Information Assurance (CS 626), 2002

[7] Montoro, R.; "LOIC DDoS Analysis and Detection", URL: http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html, 2011, Accessed December 1, 2011

[8] http://www.tenable.com/products/nessus

[9] http://www.hackerbradri.com/2012/08/cpu-death-ping-20.html

[10] Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar, Sayed Gholam Hassan Tabatabaei, "Distributed Instrusion Detection in Clouds Using Mobile Agents", Third International Conference on Advanced Engineering Computing and Application in Sciences, October 11-16, 2009 - Sliema, Malta

[11] Roschke, S., Cheng, F., Meinel, "Intrusion Detection in the Cloud", The 8th International Conference on Dependable, Autonomic and Secure Computing (DASC-09) China, Dec. 2009

[12] Aboosaleh Mohammad Sharifi, Saeed K. Amirgholipour1, Mehdi Alirezanejad2, Baharak Shakeri Aski, and Mohammad Ghiami "Availability challenge of cloud system under DDoS attack", Indian Journal of Science and Technology, Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

[13] Anjali Sardana and Ramesh Joshi, "An auto responsive honeypot architecture for dynamic resource allocation and QoS adaptation in DDoS attacked networks", Journal of Computer and Communications, July 2009, Vol. 32, P 121384-1399.

[14] Aman Bakshi, Yogesh B. Dujodwala, "Securing Cloud from DDoS Attacks Using Intrusion Detection System in Virtual Machine", Proceedings of the 2010 Second International Conference on Communication Software and Networks(ICCSN '10), P 260-264

[15] Weir, J.; "Building a Debian\Snort based IDS", URL: http://www.snort.org/docs, 2011. Accessed November 28, 2011

[16] VMware cloud, http://www.vmware.com/solutions/cloud-computing/index.html

[17] Chi-Chun Lo, Chun-Chieh Huang and Ku, J, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks". In 2010 39th International Conference on Parallel Processing Workshops.

[18] H. Debar, D. Curry, "The Intrusion Detection Message Exchange Format (IDMEF)", rfc4765, March 2007.

[19] Hisham. A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cids/

[20] Microsoft Private cloud, http://www.microsoft.com/en-us/server-cloud/private-cloud/default.aspx

[21] Open stack, http://www.openstack.org/

[22] Eucalyptus, http://www.eucalyptus.com/

[23] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, "DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks", in IEEE Transactions on Dependable and Secure Computing, under review in September 2012.

[24] http://www.ossec.net/main/

[25] "Detection of Multistage Attack in Federation of Systems Environment", Przemysław Bereziński, Joanna Śliwa, Rafał Piotrowski, Bartosz Jasiul- Military Communication Institute

[26] "OSSIM Manual", http://www.alienvault.com/documentation/index.html

[27] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, "Detecting Masquerades in Clouds through Security Events and NetFlow Data Analysis", Ready for submission to the IEEE Transactions on Dependable and Secure Computing Journal.