Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.497 – 502

SURVEY ARTICLE

IDS: Survey on Intrusion Detection System in Cloud Computing

Mr. Ashish Kumbhare, Mr. Manoj Chaudhari
Department of Computer Science & Engineering, Priyadarshini Bhagwati College of Engineering, Nagpur, India
Email: ashishkumbhare99@gmail.com, manojchaudhary2@gmail.com

Abstract—Cloud computing provides flexible on demand services to the end users with lesser infrastructural investment. Under the supervision of different managements, these services are provided over the Internet using known networking protocols, standards and formats. Existing deficiencies in underlying technologies tend to open doors for intrusion. This paper surveys different intrusions affecting basics of cloud security i.e. availability, confidentiality and integrity of Cloud resources and services. It examines proposals incorporating Intrusion Detection Systems (IDS) in Cloud and discusses various types and techniques of IDS.

Index Terms— Cloud computing, Intrusion detection system, HIDS, NIDS, DoS, DDoS, DIDS

I. INTRODUCTION

Goal of Cloud computing is to provide convenient, on-demand network access to a computing resources. Cloud provides services in various forms: Software as a Service-SaaS, Platform as a Service- PaaS and Infrastructure as Service-IaaS[6]. In this world of Internet, security and privacy of Cloud services are key issues. Data security is the greatest challenge of Cloud computing and after that intrusion detection in cloud infrastructures. Cloud infrastructure makes use of virtualization techniques, integrated technologies and runs through standard Internet protocols[19]. These may attract intruders due to much vulnerability involved in it. Cloud computing also suffers from various traditional attacks such as IP spoofing, Routing information Protocol attack, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS) etc. Firewall can be a good option to prevent outside attacks but does not work for insider attacks[12]. Efficient intrusion detection systems (IDS) should be incorporated in Cloud infrastructure. Rest of the paper is organized as follows.

II. INTRUSIONS TO CLOUD SYSTEMS

This section illustrates several common attacks (intrusions), which causes availability, confidentiality and integrity issues to Cloud resources and services.

A. Insider attack

The person who could access the whole information system with privileged authority are defined as *insider*. Insider attacks are organized and performed by these individuals to destroy or manipulate the knowledge about system or providers and include every kind of attacks which can possibly be executed from inside[11]. Authorized Cloud users may attempt to misuse unauthorized privileges. Insiders may commit frauds and destroy information or they may disclose information to others. This poses a serious trust issue[6].

B. Flooding attack

In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they are called as zombie (innocent host) [11]. Here, attacker tries to flood victim by sending huge number of packets from innocent host (*zombies*) in network. Packets can be either one of TCP, ICMP, UDP or a mix of these protocols. These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines are established everywhere over Internet. For this reason, exposition of cloud users with *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks are inevitable[8]. Flooding attacks affect the availability of serviced for authorized users. An attack that is realized to a server which serves one kind of service can prevent a vast of scale accessibility to this served service. These kinds of attacks are called DoS attacks. If servers' resources are slogged after flooding attacks and it prevents the execution of other services, which run on the server, this kind of attacks are called indirect DoS attacks[6].

C. User to Root attacks

In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system [11]. This makes him able to exploit vulnerabilities for gaining root level access to system For example; Buffer overflows are used to generate root shells from a process running as root. Buffer overflows are used for establish console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines[12].

D. Port Scanning

An attack that identifies open, closed and filtered ports on a system [11]. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning (same as ACK scan but it checks any modifications in the window field of packet) etc. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

E. Attacks on Virtual Machine (VM) or hypervisor

After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [11]. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. A zeroday vulnerability is a threat that tries to exploit application vulnerabilities that are unknown to others or the software developer. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates. Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [12]. A zero-day vulnerability was exploited in the HyperVM virtualization application which resulted in destruction of many virtual server based websites [17].

F. Backdoor channel attacks

It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hackers can control victim's resources and can make it as *zombie* to attempt DDoS attack[9]. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as *Zombie* to initiate DoS/DDoS attack. For insider attacks, signature based intrusion detection solutions can normally be used[20]. To prevent attacks on VM/Hypervisor, anomaly based intrusion detection techniques can be used. For flooding attack and backdoor channel attack, either signature based intrusion detection or anomaly based intrusion detection techniques can be used[18]. Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above.

III. INTRUSION DETECTION IN CLOUD COMPUTING

As detailed in previous section, there are different types of attacks. *Intrusion Detection Systems (IDSs)* are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection, log detected information, alert or perform predefined procedures [17, 18]. They can be either hardware or software that includes whole observed computing entities. Mainly there are three types of IDS in cloud computing systems: *Host based IDS, Network based IDS, and Distributed IDS.*

A. Host-based Intrusion Detection Systems

Host-based Intrusion Detection System was the first type of intrusion detection software to be designed, with the original target system being the mainframe computer where outside interaction was infrequent [6]. Host-based IDSs operate on information collected from within an individual computer system. A Host-based IDS monitors the inbound and outbound packets from the computer system only and would alert the user or administrator if suspicious activity is detected [5][1]. Host Based IDSs analyze the suspicious activities like system call, processes or thread, asset and configuration access by observing the situation of host. It is especially used to protect valuable and private information on server systems. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host[1]. An HIDS is not just monitor network traffic, it can also trace more and settle with local settings of an OS and log records.

B. Network-based Intrusion Detection Systems

Network-based Intrusion Detection Systems focus more greatly on the network than a specific host. Network-based IDS detects attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts[13]. Network-based IDSs often consist of a set of single purpose sensors placed at various points in a network. Network-based IDSs (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on specified points and generally located between the end point devices like routers, firewalls[1][13]. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer [1]. OSI reference model and TCP/IP model define how these layers works and manages the traffic.

C. Distributed Intrusion Detection Systems

Distributed Intrusion Detection System (DIDS) is the way of intrusion detection in a distributed environment such as grid and cloud computing [19]. All the components in the distributed area communicate each other with an agent-based approach. There are three fundamental components and assignments are similar to other types of IDSs' components. Main subject in DIDSs deal whole system like a traditional network or host [20]. DIDS components do not have a worldwide accepted standard, but there are network and host based sensor components, detection engine and management component.

D. Network Behavior Analysis Intrusion Detection

Network Behavior Analysis Intrusion Detection (NBAD) is an intrusion detection methodology which is providing to decide if the network traffic is suspicious or not by the statistical data and formal situation of network traffic[5]. Sensors detect DoS attacks with the help of to be aware of the network traffic and unexpected application services and rule violations by scanning the network[8]. Traditional NIDSs and NBAD systems share some common components like sensors and management consoles, but NBAD systems generally do not have database servers, unlike the traditional NIDSs. NBAD systems work to decide in the case of unexpected data traffic. It is generally efficient to detect DoS attacks and worms [1].

IV. CONCLUSION

The use of Cloud computing will reduce the infrastructure maintenance cost, scalability for data and applications, availability of data services and pay as you use features. Consequently, the probability of having various types of vulnerabilities causing attacks is high. This survey, discussed several intrusions which can threat integrity, confidentiality and availability of Cloud services in the future. One of the existing solutions viz. firewall may not be sufficient to solve Cloud security issues. The paper emphasized the usage of alternative options to incorporate intrusion detection techniques into Cloud.

References

[1] J. Mchugh, A. Christie, and J. Allen, "Defending Yourself: The Role of Intrusion Detection Systems", *IEEE Software*, **17(5)**, Sep.-Oct., pp. 42-51, 2000.

[2] K.V.S.N.R. Rao, A. Pal, and M.R. Patra, "A Service Oriented Architectural Design for Building Intrusion Detection Systems", *International Journal of Recent Trends in Engineering*, **1(2)**, pp. 11-14, 2009.

[3] E-Banking - Appendix B: Glossary, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ ebanking_04_appx_b_glossary.html, Accessed on: 23/02/2012

[4] Information Technology at Johns Hopkins-Glossary G-I, http://www.it.jhmi.edu/glossary/ghi.html

[5] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", *IEEE Transactions on Dependable and Secure Computing*, **4(1)**, pp. 1-15, 2007.

[6] P. Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", *IEEE 2011 World Congress on Information and Communication Technologies*, pp. 456-461, 2011.

[7] Z. Mahmood, "Cloud Computing: Characteristics and Deployment Approaches", *11th IEEE International Conference on Computer and Information Technology*, pp. 121-126, 2011.

[8] M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing", *2009 IEEE International Conference on Cloud Computing*, pp. 109-116, 2009.

[9] R. Wu, G.-joon Ahnl, and H. Hul, "Information Flow Control in Cloud Computing", *IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pp. 1-7, 2010.

[10] U. Thakar, "HoneyAnalyzer - Analysis and Extraction of Intrusion Detection Patterns and Signatures Using Honeypot", *The Second International Conference on Innovations in Information Technology*, Dubai, UAE September 26-28, 2005.

[11] H. Kozushko, “Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems”, Independent Study, September 2003.

[12] W. T Work, “Intrusion Detection Systems (IDS)”, *National Institute of Standers and Technology*, 2003, Available at: csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[13] J. Weng and G. Qin, “Network Intrusion Prevention Systems”, *JTB_Journal of Technology and Business*, pp. 37-49, October 2007.

[14] What is Intrusion Detection? Midmarket IT Security Definitions - Intrusion Detection, http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.html

[15] J. Nikolai, “Detecting Unauthorized Usage in a Cloud using Tenant”, available at: http:// www.homepages.dsu.edu/malladis/teach/717/Papers/nikolai.pdf.

[16] R. Bace and P. Mell, “NIST Special Publication on Intrusion Detection Systems”, *National Institute of Standards and Technology*, 2001.

[17] E. Cooke, “Examination of a HIDS (SNORT + ADS)”, available at: http://csc.columbusstate.edu/bosworth/CIAE/StudentPapers/cooke.edgar.pdf..

[18] “Intrusion Detection in a Cloud Computing Environment” Available at: http:// searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment accessed on February 2012.

[19] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, “A Survey on Security Issues in Cloud Computing”,Available at: http://arxiv.org/abs/1109.5388.

[20] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing”, *17th International Workshop on Quality of Service*, 2009 (IWQoS'09), pp. 1-9, 2009.

[21] K. Vieira, A. Schulter, C.B. Westphall, and C.M. Westphall, “Intrusion Detection for Grid and Cloud Computing”, *IT Professional*, **12(4)**, pp. 38-43, 2010.

[22] I. Gul and M. Hussain, “Distributed Cloud Intrusion Detection Model”, *International Journal of Advanced Science and Technology*, **34**, pp. 71-82, 2011.