IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. II (Sep – Oct. 2014), PP 32-35
www.iosrjournals.org

A Review of DOS Attacks in Cloud Computing

Vidhya.V
[1]*Department of CSE, MIT, Manipal University, Manipal, Karnataka*

Abstract: *Cloud computing is an emerging trend in the field of IT providing scalable and flexible services to the end users on demand. Cloud offers services in three levels namely infrastructure, platform and software to meet the needs of different kinds of customers. The key cloud characteristics include multitenancy, location and device independence, elasticity, resource pooling and measured service. The IT companies especially the Small and Medium Scale Businesses are moving onto the cloud which enables them to perform high end computational tasks in a cost effective manner. As more and more IT capabilities can be provided as a service in cloud, security becomes a major concern. Among the numerous attacks that can target the cloud environment, DoS or DDoS attacks can cause a major breach in security. This paper discusses the various DDOS attacks and the defense mechanisms that can be employed to secure the cloud.*

Keywords: *cloud computing, counter methods, DoS, DDOS attack, flooding.*

I. Introduction

Cloud computing is a recent technology that aims at providing access to resources instantly as per the needs of the end users. Cloud enables its customers to make use of the resources that are widely distributed in the internet to perform computations without installing in their own PC's and has to pay only for the service they consumed. All the computational requirements will be taken care of by the cloud service providers and hence all the complexities involved will be hidden from the user. NIST identifies the five key characteristics of cloud computing as on- demand self- service, resource pooling, broad network access, rapid elasticity and measured service [1]. Cloud offers services in three basic forms namely infrastructure (IaaS), platforms (PaaS) and Software (SaaS) and is on the stage of evolution to provide everything as a service (XaaS) [2].

As large magnitudes of data are moving onto the cloud, the attackers are keener to exploit the vulnerabilities associated with cloud and thereby to steal the sensitive data. Among the various threats to cloud computing, Denial of Service(DoS) attacks can prove to be the deadliest attack and even the Cloud Security Alliance has identified DoS attack as one of the nine major threats [3]. In DoS attack, the intruder overloads the target system with service requests so that it cannot respond to any further requests and hence resources will be made unavailable to its users. Distributed Denial of Service(DDoS) attack makes use of several compromised machines called zombies to launch DoS attack on the target machine and the service is disrupted or delayed [4] .DDoS attacks are getting more frequent these days and hence proper intrusion detection systems has to be deployed. This paper discusses the various kinds of DDOS attacks possible and the various countermeasures that need to be followed to avert such attacks.

II. Types of DoS Attacks

The DDoS attacks can be classified into three categories.

2.1 Volume Based Attacks/Bandwidth Based Attacks

This attack makes an attempt to overload the victim with large amounts of junk data thereby consuming the network bandwidth and resources. Examples include UDP floods, ICMP floods [5] [6].

2.2 Protocol Attacks

The attack tries to take advantage of the lacuna associated with various network protocols to overload the target's resources. Examples include Ping of Death, Smurf attack, SYN floods, fragmented packet attack etc [5] [6].

2.3 Application Layer Attacks

The attack concentrates on specific web applications and sends HTTP requests beyond the limits it can handle. This kind of attack includes HTTP DDoS attack and XML DDoS attacks or REST based attacks [6].

III. Specific DoS Attacks on Cloud

3.1 SYN Floods

This attack exploits the flaws in TCP three-way handshake procedures. A typical three way handshake includes sending SYN packet from client to server which in turn allocate the needed resources and respond to client with SYN+ACK packet and then waits for ACK from client to establish the connection. The attacker sends a series of SYN requests from a spoofed IP address and hence server will allocate all the needed resources and waits for the ACK packet from client which will never come. So the server is overwhelmed with requests thereby consuming its resources as well and will not be able to respond to a legitimate connection request [6] [7].

3.2 UDP Floods

The attacker sends a lot of UDP packets to the random ports of the target system using zombies and as soon as the target system identifies no valid applications on each port, it responds to the spoofed IP addresses by generating 'destination unreachable 'ICMP packet. The network bandwidth will be used for this unwanted reply response traffic and will not be available for the legitimate users [8].

3.3 ICMP Floods

The victim will be saturated with ICMP echo request packets by the attacker and when the victim tries to reply, the bandwidth utilization will be maximized ultimately resulting in network inaccessibility to its users [8].

3.4 Ping of Death

The target system will receive an IP packet larger than the size allowed by the IP protocol. As per the TCP/IP protocol, this packet will be fragmented at the sender side and reassembled at the receiver end. But when the oversized packet is getting reassembled, the target system will crash or its performance will be affected [5].

3.5 Smurf Attack

The attacker sends an ICMP ping message from a spoofed IP address to a broadcast IP address rather to a particular system. Hence the target system will be overwhelmed with response messages from all the systems in the network and thereby it will be prevented from responding to a valid request [5] [8].

3.6 HTTP based DoS Attack (HDoS)

The attacker uses the HTTP Get and Post request messages to flood the victim. The HTTP GET request will always try to get some information from the server and when the server is overloaded with GET requests utilizing the CPU and memory, the server or the target will be unable to respond to any further requests. The HTTP POST request is more complex as it involves input data from forms which requires more computation from the server side [4]. So HTTP POST DDoS attack is more effective than GET flood attack.

3.7 XML based DoS Attack (XDoS)

The aim of this attack is to exhaust the resources and network bandwidth of the server hosting a web service while handling SOAP messages. There are three ways to launch XDoS attack namely oversized payload, external entity references and entity expansion [9]. XDoS attacks are very easy to implement as there are very less defense mechanisms in use today.

IV. Counter Methods for DDoS Attacks

4.1 Co-operative Intrusion Detection System

A Snort based DIDS is deployed in each cloud computing region which will cooperate with each other to mitigate the effect of DDoS attack in the network. The IDS compares the type of received packet with that in its block table and if a match is found, the packet is dropped immediately. If no match is found, but detected as anomalous, alert is sent to all other IDSs. Each IDS exchange alerts with other IDS and uses the majority vote method to decide true and false alerts. If alert is true, then the block table is updated with new block rule to identify such kind of attacks in the future. The IDS consists of four components to perform the detection namely intrusion detection, alert clustering and threshold computation and comparison, intrusion response and blocking and cooperative operation [10]. The IDS helps in early detection and prevention of DDoS attack in a cloud environment with more computational time.

4.2 Cloud Trace Back Model(CTB) and Cloud Protector

The Cloud Trace Back (CTB) is used to identify the source of the DDoS attack and Cloud Protector helps to distinguish and filter these attack patterns in the future. CTB is based on Distributed Packet Marking

Algorithm (DPM) and Cloud Protector uses back propagation neural network to separate illegal message patterns. CTB is placed before the web server to avoid direct DDoS attacks [11]. The efficiency of the model depends on the efficiency of the neural network and hence training data set plays a vital role in deciding the performance of CTB.

4.3 Confidence Based Filtering(CBF) Approach

This approach works on two periods namely a non-attack period and an attack period. During a non-attack period, it identifies unique correlation patterns among legitimate packets by extracting attribute pairs in their IP and TCP headers. Then it calculates a confidence value to determine the trustworthiness of a particular correlation pattern between an attribute pair. Higher the frequency of an attribute pair during normal packet flow, the higher the confidence value it can get. This dataset can be called as a nominal profile. During an attack period, CBF score for each packet is calculated which is the weighted average of confidence values of attribute pairs in it. Then the CBF score is compared with discarding threshold to decide whether the packet is legitimate or not. If CBF score is higher than the threshold, the packet is legitimate and allowed to pass or else the packet is discarded [12]. The merits of CBF method includes less storage space and high computational speed and efficiency which makes it suitable for large network traffic.

4.4 . CLASSIE Packet Marking Approach

CLASSIE is an IDS based on decision tree classification system which helps to prevent HX-DoS attacks, a combination of HDoS and XDoS attacks. CLASSIE is placed in one-hop distant from the host and uses it rules set to identify malicious packets. The packets will be marked after evaluation by CLASSIE and marking will be carried out by edge and core routers. The Reconstruction and Drop (RAD) which is placed one-hop back from victim makes the decision whether to allow or drop the packet. Thus the malicious packets will be marked at the attacker's end and dropped at the victim's end [13]. This method significantly reduces the overhead in packet marking and false DoS attack rates.

4.5 Filtering Tree Approach

This approach is very useful to curb HDoS and XDoS attacks in application layer. The client request is converted to XML format and then the SOAP message is doubly signed and embedded with client IP address, client puzzle and puzzles solution. Then the SOAP message is forwarded to IP trace back which compares the incoming IP address with that stored in its table. If a match is found, the packet is discarded or else it is forwarded to Cloud Defender. The Cloud defender filter the attack packets with the aid of five filters namely sensor filter, hop count filter, IP Frequency Divergence Filter, Puzzle Resolver Filter and Double Signature Filter [14]. The method fails to identify DDoS attacks in transport and network layers of the cloud.

4.6 Information Theory Based Metrics Method

This method works in two phases, behavior monitoring and behavior detection. In the first phase, normal web user behavior is identified during non-attack period and an entropy value for requests per session is calculated and a trust score is assigned to each user. During behavior detection phase, the entropy value for each request is calculated and compared with a threshold value. If it exceeds the threshold value, then the request packets are considered malicious and dropped immediately. If calculated entropy is less than threshold, and then based on the trust score of the user and difference in entropy value, the rate delimiter restricts the user access. To manage the workload of the system, a scheduler is also put into use [15].Table 1 show the summary of various approaches used to avert DDoS attacks.

Table 1: Summary of approaches to avert DDoS attacks in cloud

S.No	Method	Features	Limitations
1	Co-operative IDS	1.Avoids single point of failure attack 2.Improved reliability compared to pure Snort based IDS	Takes more computational time than pure Snort based IDS
2	Cloud Trace back Model	1.Averts direct DDoS with CTB 2.identity of attacker will be made known during successful DDoS attack	1. Collecting proper training data set for neural network is difficult. 2.Performance depends on accuracy of training data set
3	Confidence Based Filtering Approach	Small storage size for nominal profile and high packet filtering efficiency	Does not have high accuracy than other approaches.
4	CLASSIE Packet Marking Approach	1.Identifies HX-DoS attacks 2.Reduces false positive rate of DoS attacks	Helps to identify only application layer DDoS attacks.
5	Filtering Tree approach	1.Uses double signature les to	Can detect only application layer

		avoid XML rewriting attacks and client puzzles to detect HDoS attack 2.Filters attack in several stages	DDoS attacks
6	Information Theory Based Metrics Method	1.uses the concept of entropy 2.Easy to implement and low false packet rejection rate	Chance of information loss due to aggregation in entropy

V. Conclusion

Cloud computing revolutionize the way how internet is used by providing everything as a service on a pay per usage basis. Even though cloud offers a multitude of benefits to individuals and organizations, cloud is under high risk of attack and one such attack that can cause a major breach in security is DoS or DDoS attack. This paper gives an idea of the various kinds of DoS attacks that can happen in a cloud and the various approaches that can be used to protect the cloud to detect and prevent DDoS attacks.

References

[1]. National Institute of Standards and Technology-Computer Security Resource Center. www.csrc.nist.gov

[2]. Nikhil Nischal and Peeyush Mathur, Cloud Computing: New challenge to the entire computer industry,IEEE 1st International Conference on Parallel, Distributed and Grid Computing, 2010.

[3]. The information week website.http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085

[4]. K.Shanti, A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.

[5]. S.S. Chopade, K.U. Pandey, D.S. Bhade, Securing Cloud Servers against Flooding Based DDOS Attacks, in Proc. International Conference on Communication Systems and Network Technologies,2013.

[6]. DDoS Attack. http:// www.incapsula.com/ddos/ddos-attack

[7]. T.Siva, E.S.Phalguna Krishna, Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, International Journal of Engineering Trends and Technology (IJETT), vol. 4, May 2013.

[8]. B. Prabadevi, N.Jeyanthi, Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey, IEEE Explore, 2014.

[9]. Amit Vinayakrao Angaitkar, Narendra Shekokar, Mahesh Maurya, The Countering the XDoS Attack for Securing the Web Services, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , pp.3907-3911,2014.

[10]. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, 39th IEEE International Conference on Parallel Processing Workshops, 2010, pp280-284.

[11]. Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, Securing Cloud Computing Environment Against DDoS Attacks, IEEE International Conference on Computer Communication and Informatics, 2012.

[12]. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.

[13]. E.Anitha, Dr.S.Malliga, A Packet Marking Approach to Protect Cloud Environment against DDoS Attacks, International Conference on Information Communication and Embedded Systems, 2013.

[14]. Tarun Karnwal, T.Sivakumar, G.Aghila, A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack, IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012, vol-01, pp-9-12.

[15]. S. Renuka Devi and P. Yogesh, Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics, CS & IT-CSCP 2012, pp.217–223.