Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Distributed Denial of service Attacks on Cloud Environment

Ruchi Mehta
Institute Of Technology
Nirma University

Abstract: Security in this world of digital computing plays a typical role, since all the operations are automated and large volumes of data are being maintained in the servers. Cloud computing is one of the evolving technologies where a huge volume of storage is made on-line, data and services are also distributed. Because of its distributed nature, they have become easy targets for the intruders to exploit the information. The wellknown Distributed Denial of Service (DDoS) attack is the most prominent attacks in this area of computing. DDoS is the single largest threat to internet and internet of things. This paper provides a wide survey on various DDoS attacks, their vulnerabilities and countermeasures proposed against them. Also this paper provides an in-depth analysis on effects of DDoS attacks in the Cloud environment. Through the analysis done it will be useful for designing a secured cloud infrastructure which will abide the DDoS attacks.

I. INTRODUCTION

Cloud computing is group of computers networked together in same or different geographical locations, operating together to serve many consumers with different need and workload on demand basis with help of virtualization. Cloud computing is the most user friendly way for the consumers to deal with theirneeds uniquely through internet. User just needs a browser with internet connectivity to avail the many cloud services. Most widely used now a days popular cloud services are Gmail, Facebook, Dropbox etc are all can be accessed through browser having internet connectivity anywhere through laptop
, cell phones or tablet etc with any modes of mobility [1].
The cloud infrastructure is fully virtualized to utilize hardware through remote serves and huge database as datacenter. One of the major advantage of cloud computing is that cloud infrastructure and its maintenancewill betaken care by the third party or cloud service provider on their own cost. This point is basically allured many big IT industries and other industries to adopt cloud computing for their organization to reduce their IT cost. But still most of the industries have lack of confidence on cloud computing because they are prone to security threats and they cannot take chance with their loss of data.
As cloud computing provide so many benefits to the user at the same time it provides facility to attackers. With the help of DDOS attacks attacker make the target server or any resource so saturated that it is not in a position to provide stable service to its consumers. Sometimes DDOS proves so threateningthatitcancauselossofdatainorganizationandloss of huge computational cost as cloud rely on pay per use utility.

A. Distributed Denial Of Service Attack

A denial of service is characterized by an explicit attemptby an attacker to prevent authenticate users from using computing resources. An attacker may attempt to: flood a network and thus reduce a legitimate user's bandwidth, disrupt service to a specific system and a user prevent access to a service [2]

B. Impacts ofDDoS

The attacker sends a huge amount of badrequesttoone target victim or certain service. The impact of such a flooding attack is expected to be amplified drastically. Now we discussed different kinds of impact [3]

1) Direct Denial of Service: When the Cloud Computing operating system notices the high workload on the particular service; it will start to give more computational power like virtual machines, service instances etc. to cope with the additional workload. Cloud protection systems try to work against theattacker.

2) Indirect Denial of Service: Depending on the Computational power in control of the attacker, side effect of the direct flooding attack on a Cloud service potentially consists in that other services provided on the same hardware servers may suffer from the workload caused by the flooding. Thus, if a service happens to run on the same server with another, flooded service instance, this can affect its own availability as well[3]

3) Accounting Cloud computing: service is charging the customers according to their actual usage of resources ,another major effect of a flooding attack on a Cloud service is raising the bills for Cloud usage drastically. The problem is there are no upper limit s to computational power usage [3]

C. Elements ofDDOS

- **Victim (Target)** receives the brunt of the attack.
- **Attack Daemon Agents (Zombie)** Agent programs that actually carry out the attack on target victim. Attackers gain access and actually conduct the attack on victim. Daemons affect both the target and the host computers
- **Master Program/Agent)**coordinates the attack through the attack daemons also known as handler.
- **Attacker/Attacking Hosts** Mastermind behind theattack using the master, which stays behind the scenes during real attack, which makes it difficult to trace. Todoall this attacker has to work hard on it he/she need to study the network topology and bottleneck that can be exploited during the attack

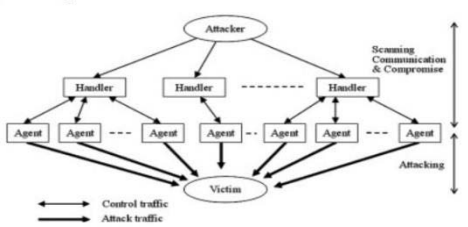

Figure 2: Components of Distributed Denial of service attack and steps take place during the attack.

1) The real attacker sends an execute command to master program.

2) The control master program receives the execute message and propagates the command to the attack daemons under itscontrol.

3) Upon receiving the attack command, the attack daemons begin the attack on the victim.

4) : Then the victim site goes down and not available to give services to its intended user.

D. Methods of DDoS

These are the method which is used for denial of service attack

1) **Smurf-attack** involves an attacker sending a large amount of Internet Control Message Protocol (ICMP) echo traffic to a set of Internet Protocol (IP) broadcast addresses.

2) **SYN Flood attack** is also known as the Transmission Control Protocol (TCP) SYN attack, and is based onexploiting the standard TCP three - way handshake. The server being unable to process because of incoming connection queue gets overloaded [4].

3) **UDP Flood attack** is based on UDP echo and character generator services provided by most computers on a network. The attacker uses UDP packets to make connect ion to the echo service on one machine to the character generator service on another machine. There is another method like Teardrop attack, Land attack, Flood attack, Fraggle attack, Ping of death attack , Buffer overflow attack used by attacker to launch DDOSattack [10].

E. Technique used by attacker

Distributed denial of service methods employed by an attacker. These techniques help an attacker coordinate and execute the attack [7]. The techniques are listed in chronological order.Itcanbeobservedthatastimehaspassed,thedistributed techniques (Trinoo, TFN, Stacheldraht, Shaft, and TFN2K) have become technically more advanced and more difficult to detect[4].

II. DEFENCES AGAINST D DOSATTACKS

Many observers have stated that there are currently no successful defenses against a distributed denial of service attack, but there are numerous safety measures that a host ornetworkcanperformtoincreasethesecurityofnetworkand neighboringnetworks [10]. Two features that hinder the advancement of defense technique. First, the source of DDOS attacks are very difficult to find in distributed environment. It's difficult to find out the real attacker because he/she can use the multiple layer of control master program [9]. Second, it's very hard to distinguish between normal traffic and DDOS attack traffic. Attacker generate same request as legitimateuser and we don't have effective differentiation mechanism. There are some distributed defense frameworks that provide defense against DDOSattack:

1) **Filtering Routers:** Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks. Many people assume that routers, which use access control lists (ACLs) to filter out "undesirable" traffic, defend against DDOS attacks. ACLs can protect against simple and known DDOS attacks, such as ping attacks, by filtering unwanted, unknown protocols and also prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on allrouters.

2) **Load Balancing:** It is used to implement failover - The continuation of service after the failure of one and more components. These components work under controlled supervision, when become non responsive, theloadbalancerinformed and stop sending traffic to it. Through the use ofload balancer we can minimize the resource consumption, keepcost low and also enablescalability [8].

3) **Disabling IP Broadcasts:**By disabling IP broadcasts, the host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. To defend against this attack, all neighboring networks need to disable IP broadcasts [4].

4) **Audit:**It means to watch what happened in cloud system. It could be added as an extra layer above the virtualized operating system to monitor what happen in the network.Main attribute should beaudited:

Logs: Information about run time environment and user application

Events: Thechange of state and other factor that affect system/services availability.

Monitoring: It must be restricted to what the cloud providers reasonably need in order to run their facility [5].

5) **Applying Security Patches:**To guard against denial of service attacks, host computers must be updated with latest securitypatchesandtechniques.Forexample,inthecaseofthe SYN Flood attack, there are three steps that thehostcomputerscan take to guard themselves from attacks: increase the size of the connection queue, decrease the timeout waiting for the three-way handshake, and employ vendor software patches to detect and circumvent the problem [7].

6) **Disabling Unused Services:**If UDP echo services are not required, disabling them will help to defend against the attack. If one computer opens 50 ports, the attacker can use these ports to launch different DDOS attack. If only two ports are opened the attack type will be restricted [6]. The services should be disabled to prevent attacks if network services are unneeded orunused.

7) **Performing Intrusion Detection:**By performing intrusiondetection,ahostcomputerandnetworkareguardedagains t being a source for an attack, as while as being a victim of an attack. It is a device or software application thatmonitors network or system activities. If they found malicious activities or policy violations, the produces reports to a management station. Network monitoring is a very good pre-emptive way of guarding against denial of service attacks [8]. By

monitoring trafficpatterns,anetworkcandeterminewhenitisunderattack, and can take the required steps to defend itself [4].

III. CONCLUSION

No doubt the recent advancement in the field of cloud computing technology proved to be very helpful to many industries and individual consumers in terms of availing various services through internet across globe but security threats pose a great challenge to leading industries that are totally willingto migrate their IT resources in cloud environment. DDOS attack proves extremely threatening by looking at the consequences whichcauseshugedataleakageandfinanciallosstoindustries.
Also time and cost involved to fix these issues are very high which is quite enough reasons to moral down the confidence of many industries whom are totally intended to rely on cloud infrastructure.

REFERENCES

[1] Vincent Shi-Ming Huang , Robert Huang and Ming Chiang, A DDoS Mitigation System with Multi-Stage Detection and Text-Based Tur- ingTesting in Cloud Computing, 27th International Conference on Ad- vanced Information Networking and Applications Workshops,IEEE2013

[2] Felix L au, Stuart H. Rubin, Michael H.Smith Distributed Denial of service attacks IEEE, 2000.

[3] Meiko Jensen, Jorg Schwenk, Nil Gruschka On technical issues in cloud computing, IEEE International Conference on cloud computing, 2009.

[4] Felix L au, Stuart H. Rubin, Michael H.Smith Distributed Denial of service attacks IEEE, 2000.

[5] Minqi Zhou, Rong Zhang, Wei Xie Security and Privacy in Cloud computing: A Survey sixth International Conference on Semantics,2010.

[6] Lin Jingna An analysis on DOS attack and defense technology seventh International Conference on Computer Science, Melbourne, Australia, July 14 - 17, 2012.

[8] Minqi Zhou, Rong Zhang, Wei Xie Security and Privacy in Cloud computing: A Survey sixth International Conference on [7] Ping Du, Akihiro Nakao, DDOS defense as a Network service IEEE, 2010.Sameera Abdulrahman Almulla, chan Yeob Yeun, Cloudcomputing security management,IEEE, Semantics,2010.

[9] Dimitrios Zissis, Dimitrios Lekkas Addressing cloud computing security issues, University of the Aegean, Syros 84100, Greece IEEE Dec 22, 2010

[10] http://www.bankinfosecurity.com/bank-attacks-7-steps-to-respond-a- 5221