A Review: Denial of Service and Distributed Denial of Service attack

Sandeep Kaur
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: sandeepkaur097@gmail.com
Rakesh Kumar
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email:rakeshkumar@kuk.ac.in
Girdhar Gopal
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: girdhar.gopal@kuk.ac.in

---Abstract---

Denial of Service and Distributed Denial of Service attack has become major security issue to the current computer networks. Both DoS and DDoS are used to make a web resource or site unavailable to its genuine users. However the motive, target and method of DoS attack may vary. These attacks generally consist efforts of a person or machine to temper normal functionality of any internet server or host.The objective of this paper is to provide a survey of various methods of distributed denial of service attacks, its detection and some approaches to handle these attacks.

Keywords: DoS, DDoS Attack, Security, Vulnerability

1. Introduction

World Wide Web (WWW) leads an impact all around the world because every information is available on web. A web application is defined as any program run on Internet to provide web services. Web applications are used to manage and process a wide range of critical information including information of corporations, customers, organizations and countries. This information must be stored securely while maintaining reliability and availability.

Web applications are vulnerable to security attacks. These vulnerabilities are growing with the rapidly increasing number of users on Internet. One of the most common vulnerability is Denial of Service attack.

1.1 Denial of Service attack (DoS)

Denial of Service attack is a well known attack technique to prevent a web application from serving to its genuine users. DoS attack as its name implies basically means refusing services target network or application. DoS attack is launched by a single host or system.Two most common methods used by DoS attacker to launch attack are [1] by exploiting web application vulnerabilities or weakness in Internet protocols (vulnerability/logic attack). For instance logic attack is LAND attack or by sending a huge amount of malicious traffic towards victim (flooding attack). Example of flooding attack is TCP/SYN flooding attack. Flooding attacks can target a particular web application by consuming its key resources like CPU, memory or I/O bandwidth. They can also disturb normal functioning of any network by consuming its all available bandwidth.

1.2 Distributed Denial of Service attacks (DDoS)

DDoS attacks are advance form of DoS attack. When attack traffic comes from multiple resources, residing at different locations then this type of attack is called DDoS attack. DDoS attack has a large number of compromised hosts called Zombies in a controlled manner to launch the attack.

According to CIAC (Computer Incident Advisory capability), the first large scale DDoS attack incident was occurred in 1999. After that in February 2000, DDoS flooding attack hit Yahoo [2], October 2002, DoS attack was performed on DNS root servers 9 out of 13 Domain Name servers disturb services for an hour because of

DDoS attack [3]. In [4] February 2004, MyDoom attacked approximate 1 million computers. in July 2009, a similar type of attack was launched against [5] government media websites of South Korea and the United State. On August 2009, social networking sites Facebook , twitter and Google blogging pages were under DoS attack due to which Twitter becomes unavailable and Facebook restore its services. These DDoS attack mostly uses flooding of SYN, TCP, UDP or ICMP packets. [6] From 2010 to 2012 there was an increase in application based attacks. Reflective attacks are active from 2013 and have playing a major role in enterprise security.

1.2.1 DDoS attack strategy: DDoS is a multisource attack in which millions of compromised hosts work in a coordinated fashion to achieve a predetermined goal. For launching DDoS attack basic elements are:

Attacker: Initiator and Controller of whole attack process.

Master: Injected hosts work as master of other compromised hosts.

Zombies/agents: Compromised host that is controlled by real attacker and responsible for sending malicious traffic towards victim. Number of zombies present decides the size of Botnet which in turn decide the scale of attack. There can be thousands or millions of zombies participating in a single DDoS attack.

Botnet: A whole group of zombies is called Botnet. Botnet decide the size or scale of attack, as number of zombie's increases attack becomes more powerful and disastrous.

Victim: Target of attacker.

1.2.2 How DDoS attack works: DDoS attack is carried out in two phases: Firstly, an attack network is build by an attacker having thousands or millions of compromised agents called zombies or bots. Then these bots send a large number of malicious traffic towards targeted host either under the command of attacker or on the trigger of any event.

Building of Attack network: Depending upon the scale and effect of attack, attacker compromise hosts. For compromising attacker scan for poorly secured systems; this process is called scanning. After scanning process malicious codes are installed on identified systems to compromise them. These compromised hosts further scan for vulnerable systems, this self propagation nature helps in building a large scale attack network having thousands of compromised hosts.

Attack process: Attacker is the master of these compromised hosts; whole attack process is controlled by it. Attacker sends commands to zombies (compromised hosts) to launch attacks. Communication between attacker and zombies uses protocol such as HTTP, IRC and ICMP.

2. Categorization of DDoS attack

There are three main [7] Categories of DDoS based on how they affect the victim are:

Volumetric attacks are used to exhaust the bandwidth of victim's network. In this type of attack large volume of traffic is send towards victim to consume its bandwidth. The effect of these attacks is measured in Bps (bit per second).

Protocol based attacks consumes actual server resources such as firewall and load balancers. The size of the attack is measured in Packet per second.

Application based attacks target a particular application. The aim is to consume available resources of web server to make it unuseful. Measure for the attack is Request per second.

Based on traffic generation method used DDoS attack can be:

Direct DDoS attack: Direct DDoS attack [8] in which attacker directly sends large number of attack packets to victim. These packets can be ICMP, UDP or combination of both.

Reflector DDoS attack: Reflector attack uses intermediate nodes known as reflectors as attack launchers. Attackers send packets to reflector with spoofed IP address. Without realizing this packets are malicious reflector forward packets to victim. IP traceback do not work for these attacks because of IP spoofing.

IJSER

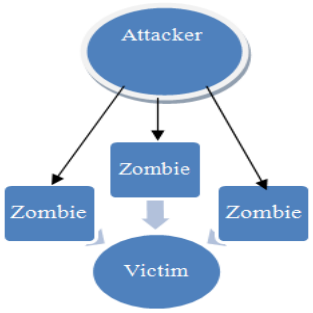

Fig. Direct Flooding attack

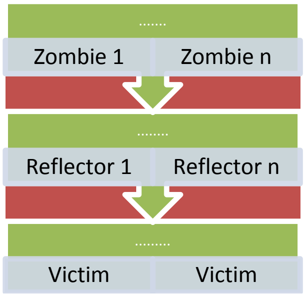

Fig. Reflector DDoS attack

IJSER

Some specific type of DDoS attacks are:

TCP SYN flooding attack: A TCP SYN attacks in which attacker abuses the three way handshake working of TCP protocol. In a normal TCP connection, first Client sends a SYN message to server. The server then replies the message by sending SYN+ACK of that request to the Client. The client then finishes connection establishment by responding with an ACK message.
In TCP SYN attack attacker sends many fake SYN requests to Server and does not reply to SYN+ACK required for completing connection. Server now has a large volume of half open connections which consume its available bandwidth and make it unreachable.

ICMP flooding attack: In ICMP flooding, attackers send large volume of ICMP_ECHO requests to victim. Victim then reply to each ICMP_ECHO request. Victim is now busy in responding an unnecessary request. It consumes its available resources and bandwidth. This in turn causes crash or unavailability of victim. Rate limiting mechanism works well for these attacks

UDP flooding attack: UDP is a connectionless protocol. It does not require any handshake to establish connection between client and server. Attacker sends a high volume of UDP packets towards victim. This useless traffic exhaust victim's resources, which in turn reduces the bandwidth amount available for legitimate users on the system.

Smurf attacks: In Smurf attack attacker broadcast ICMP_ECHO requests in the network with spoofed IP address of victim as source address. Receiver of these requests then sends ICMP_ECHO reply to source address which is victims address actually. Victim's capacity becomes zero due to these unnecessary replies. These attacks can be handled by simply blocking broadcast of ICMP_ECHO requests or by deploying ingress filter at source node.

Ping of Death attack: Ping of death sends many Ping requests continuously with oversized packet to the victim that will lead to unavailability or shutdown of victim machine.

Teardrop attack: Whenever data travel over the internet, it is fragmented at the source and reassembled at the destination. Teardrop attack sends oversized payloads with corrupted IP fragments to the victim machine.

3. DDoS Defense

DDoS attack waste a lot processing time, resources and memory etc. DDoS defense is to detect the attack as soon as possible and to completely remove or reduce the impact of this attack. Several DDoS challenges against the design of successful defenses mechanism are:

Involvement of large number of agents in attack process: Distributed denial of service attack uses large number of compromised hosts distributed at different locations building an attack network. All attack agents are difficult to trace and even if traced it is more difficult to decide what action could be taken against these thousands of attacker agents.

IP Spoofing: Use of fake identity in IP source address of any packet is called IP Spoofing. Attackers frequently use source address spoofing to conceal their identity. Because of IP spoofing it is difficult to trace true attacker. Since tracing is impossible this greatly encourages DDoS attack incidents. Due to hidden identity these compromised machines can be reused for future attacks.

Similarity between attack traffic and genuine traffic: Attacker sends large volume of traffic to overload victim computer. This attack traffic has similar characteristics as normal ones. Since it is difficult to decide which one is attack traffic, which one is original?

3.1 DDoS Defense mechanism

Based on time of the defense activity [9] deployed on network or application DDoS defense can be:

3.1.1 Preventive defense methods: This mechanism works before the happening of attack. Preventive measures can eliminate the effect of attack by several general methods such as allowing connections to trusted users only or eliminating out of band signaling. Mitigating effect of attack on victim by allocating it sufficient amount of resources so that it can survive under attack conditions or by installing effective security patches on system.

IJSER

3.1.2 Reactive defense methods: Reactive methods try to reduce the effect of attack on victim. For this they need to detect the attack and then react to it.

Detection: Detection of attack can be signature based or anomaly based:

Signature based detection store the signature of known attack in a database and monitor the incoming and outgoing traffic for the presence of these patterns. If any match is found packets are simply dropped. This method works only for known attacks patterns, new attacks remains undetected.

Abraham Yaar et al. proposed a Pi (Packet Identifier) [10] mechanism in which signature of each packet is stored in each packet. Each packet traversing same path have same signature ID. Based on these signatures filtering of attack packets is performed. Positive point of Pi is that it works well under large scale DDoS attack and effective even when half of routers are involved in packet marking. Limitation of Pi is that collision can occur; same path information can point different paths. StackPi [11] an improvement of Pi also uses packet marking and filtering scheme to propose an algorithm. This method solve IP spoofing problem by using 16 bit identification field in IP header on Packets to mark the path traveled by packets. Packets having same path would have same marking. Collision is the main limitation of this approach. Anomaly based detection scheme have a model of normal system behavior with which current system behavior is compared to detect attacks. This technique can effectively detect previously unknown attacks.

Mitigation: After detection of attack mitigation strategies are used to reduce the impact of attack on victim. Based on mitigation techniques reactive mechanism can include agent identification, rate limiting or filtering etc. In Agent identification source of attack is identified and obtained information is used for further processing .Example of agent identification scheme is IP traceback techniques.

Trace back in DDoS defense is finding the real origin/source of attack by traversing the path traversed by attack packet in reverse direction. Finding real attacker helps in attack mitigation. However implementation of trace back has several problems which make them infeasible such as IP spoofing, stateless IP routing where path is not complete etc. Some IP traceback methods proposed in past are described here:

PPM (Probabilistic packet marking) scheme which uses assumes that attack packets come more frequently than other packets [12]are used to identify the real identity of attack source. In this packet marking scheme each router through which data packet pass probabilistically attach its IP address in packets; this attached information is used for reconstruction of paths. PPM is only useful for direct DDoS attacks. In case of reflector or distributed attacks invalid path can be constructed. It also increases computational overhead on intermediate routers. One major disadvantage of this packet marking scheme is that routers can also be compromised by sending many requests at a time. One another approach to overcome the limitations of PPM scheme is purposed called DPM (deterministic packet marking) which marks all the packets at ingress interfaces. In deterministic packet marking [13] scheme most of the processing is done at the victim. DPM can work for reflector DDoS which was the limitation of PPM scheme. It reduces computational overhead on routers by marking packets at first ingress router only. It also requires few packets to reconstruct path. DPM uses 16 bit of identification field of IP header with one bit for marking information. This identity information as packet travels throughout network. Main difference between DPM and PPM schemes is DPM only marks packets at only first ingress router while PPM marks at all routers at path. Rate limiting mechanism is applied on packets identified by detection mechanism to reduce the impact of attack on victim. Ingress/Egress filters are used to filter out the attack traffic completely. Filtering rate limit the unwanted traffic reduces impact of attack on victim. Example of [14] Filtering mechanism is firewall or Intrusion detection system. Packet Filtering is used for reducing the impact of flooding attacks. P.Ferguson and D.Senie uses ingress/egress filtering techniques to detect the attack traffic having spoofed source IP addresses. Due to these spoofed addresses victims can not differentiate between attack packets and real ones. Ingress/Egress filtering detects and filter spoofed IP addresses. This approach greatly reduces attack power but limitation is processing overhead and requirement of installing filters on all routers [14]. X.Liu has uses StopIt servers to block unwanted traffic. Source identity is included in packets to stop spoofing attack. But attack on StopIt server is also possible. Authentication requirement and deployment of StopIt server are major limitation of this method [15].D-WARD a source end defense monitors both incoming and outgoing traffic, aims to detect any abnormal activity. D-WARD works as a firewall to analyze and stop attack traffic. D-WARD monitors incoming and outgoing traffic and compare them with some predefined signature values. Attack packets are dropped if any mismatch is found. It defines normal flow signature database for each type of traffic with which flow of recent traffic is matched. Consumption of memory space and CPU cycles are major limitations of D-WARD.

4. Conclusion

The last decade has observed an exponential growth of WWW (World Wide Web) due to common trend of migrating each & every information on the web. In parallel, there is an exponential growth of attacks on web applications, making sometimes life measurable of end user. Some common attacks are SQL injection, XSS, DoS, DDoS, authorization and authentication attacks etc. In this paper an exhaustive survey of DoS and DDoS is carried out to analyze the modus operandi of attackers and to examine the detection, prevention mechanisms used in past, so that an exhaustive set of guidelines can be provided and a framework may be designed to make the application full proof against such attacks.

IJSER

References

[1] D. Moore, G. M. Voelker and S. Savage, "Inferring Internet Denial of Service activity," *ACM Trans. Comput. Syst.*, vol. 24, no. 2, pp. 115-139, 2006.

[2] "Yahoo on Trail of Site Hackers," 2000. [Online].Available: http://www.wired.com/news/business/0,1367, 34221,00.html.

[3] "Powerful Attack Cripples Internet," 2002. [Online].Available: http://www.greenspun.com/bboard/q–and–a–fetch–msg.tcl?msg_id=00A7G7.

[4] "Mydoom lesson: Take proactive steps to prevent DDoS attacks," 2004. [Online]. Available: http://www.computerworld.com/s/article/8993

2/Mydoom_lesson Take proactive steps to prevent DDoS_attacks?taxonomyId=017.

[5] "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy," 8 July 2009. [Online]. Available: http://www.guardian.co.uk/media/2010/dec/08/operation–payback–mastercard–website–wikileaks.

[6] "GLOBAL APPLICATION & NETWORK SECURITY REPORT," 2015-2016.

[7] "ddos-attacks," [Online]. Available: https://www.incapsula.com/ddos/ddos-attacks/.

[8] M. Aamir and M. A. Zaidi, "DDoS Attack and Defense: Review of Some Traditional and current techniques," 2014.

[9] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, pp. 39-53, 2004.

[10] A. Yaar, A. Perrig and D. Song, "Pi: A Path Identification Mechanism to Defend against DDoS Attacks," *IEEE Symposium on Security and privacy*, p. 93, 2003.

[11] A. Yaar, A. Perrig and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 1853-1863, 2006.

[12] K. Subhashini and G. Subbalakshmi, "Tracing Sources of DDoS Attacks in IP Networks Using Machine Learning Automatic Defence System," *International Journal of Electronics Communication and Computer Engineering*, vol. 3, no. 1, pp. 164-169, 2012.

[13] A. Belenky and N. Ansari, "IP Traceback With Deterministic Packet Marking," *IEEE*, vol. 7, no. 4, pp. 162-164, 2003.

[14] P. Ferguson and D. Senie, "Network ingress filtering: defeating denial of service attacks that employ IP source address spoofing," 2000.

[15] X. Y, Y. Lu and X. Liu, "To filter or to authorize: network-layer DoS defense against multimillion-node botnets," in *ACM SIGCOMM conference*, NY,USA, 2008.

IJSER