International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 2, February- 2013

Distributed Denial Of Service: Attack At Application And Transport Layers And Precautions

G.N.K.Suresh Babu and Dr.S.K.Srivatsa

Associate Professor - GKM College of Engineering and Technology, Chennai

Sr.Professor – St.Joseph's College of Engineering, Chennai.

ABSTRACT

The frequency of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are rapidly increasing. (DDoS) attack has the significant ability of concealing the traffic because it is very much like normal traffic. The Internet is part of the critical national infrastructure but is unique in that it has no customary borders to safeguard it from attacks. Network security becomes critical part in the internet world. Attacks that are seen everyday on the Internet include direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. Specific attacks directed at a service provider's infrastructure can be very damaging and cause wide spread outages.

In this paper we describe DDoS attacks in the application layer and transport layer of the OSI model and precautions to avoid the attack.

***Keywords** : Loris, Network Layers, Anti Virus, Firewalls, Internet*

1 INTRODUCTION

Making of internet or network resource unavailable for intended users is the Distributed Denial of Service (DDoS).The Distributed Denial of Service (DDoS) attack are done indirectly by the attacker and the attacker control the system remotely. One common way of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Denial-of-service attacks can also lead to problems in the network around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by an attack, compromising not only the intended computer, but also the entire network. Figure 1 illustrates the why Distributed denial of Service (DDoS) is threat to the internet. Every layer of communication has its own unique security challenges. Some of the layer in the OSI model is vulnerable for the Distributed Denial of Service (DDoS). Application layer DDoS attacks are increasing rapidly representing as much as a quarter of today's DDoS attack. Transport layer is also vulnerable to the distributed denial of service.

In section 2 we describe about Distributed Denial of Service (DDoS) attack in different layers of the OSI model. In section 3 we describe about the precautions to take to avoid the Distributed Denial of Service (DDoS) attack and finally Conclusion.

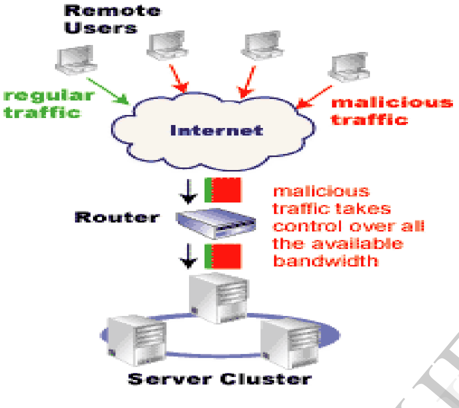

Figure 1 : Attack of DDoS

2 ATTACK IN DIFFERENT LAYERS

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks. A bandwidth depletion attack is aimed to flood the victim network with malicious traffic that prevents legitimate traffic from reaching the primary victim. Figure 2 DDoS attack observed by Kaspersky Lab across the countries.

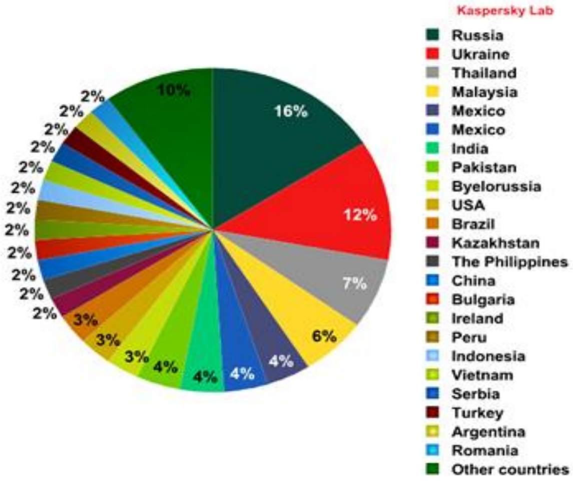

Figure 2: DDoS attack across the countries

A resource depletion attack is an attack that is aimed to tie up the resources of a victim system making the resources unavailable for intended users.

2.1 APPLICATION LAYER

Application layer DDoS attacks are increasing rapidly representing as much as a quarter of today's DDoS attack. The three application layer attacks are slow loris , slowPost and SIP INVITE Flood. Figure 3 illustrates the average monthly Mbps attacks.

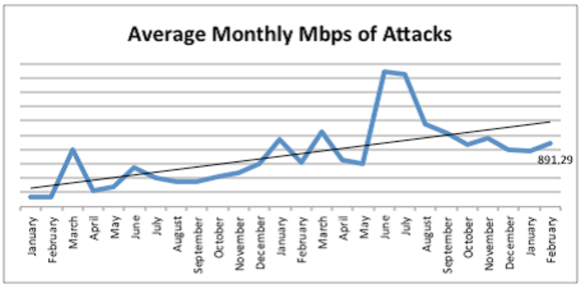

Figure 3: Average Monthly Mbps Attacks

a) Slow loris

It basically uses a concept of keeping an HTTP session alive indefinitely (or as long as possible) and repeating that process a few hundred times.

Typical flooding attacks require tons and tons of packets and end up denying service to other applications as a result. By creating a flood of TCP requests, sure you can take down an upstream router, or a web server, but it’s overkill if you really just want to take down a single website. Slow loris does this without sending an overabundance of TCP or HTTP traffic, and it does so without increasing the load significantly, or in any other way hurting the box (assuming other things aren’t tied to the HTTP processes - like a database for instance). This appears to only affect certain types of web servers (generally those that thread processes, like Apache, but not like IIS). Figure 4 shows the observed highest attack by kaspersky lab.

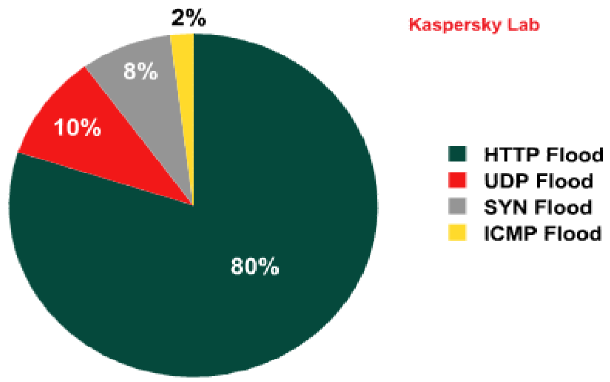

Figure 4:Highest attack

b) Slow Post

Slow HTTP POST Distributed Denial of Service (DDoS) tool simulates an attack using POST headers with a legitimate "content-length" field that lets the Web server know how much data is arriving. Once the headers are sent, the POST message body is transmitted slowly, thus gridlocking the connection and server resources.

Slow HTTP attacks are gaining in popularity among the bad guys as a way to quietly wage a DoS attack because these exploits are relatively easy to perform, require minimal computing resources, and often are tough to detect until it's too late.

c) SIP INVITE Flood

The two attacks above both target HTTP; this one is a VoIP flood that targets SIP. It takes advantage of the normal time lag during the SIP call initiation process to overload a SIP server. Since SIP runs over UDP, a single packet from a caller, hacker, or botnet can start the process of dialing and ringing at the beginning of a phone call. In our everyday lives, we don’t think anything of the 20 second delay between entering a phone number and hearing hello or the voicemail prompt from the other end. But that delay, when multiplied across thousands of simultaneous connections can crash a server and potentially open the door for even more within VoIP-based call center. Plus, its very difficult to determine in advance which calls are legitimate and which ones are part of a Distributed Denial of Service (DDoS) ,especially if an attacker is clever enough to spoof the IP addresses in UDP headers, or to spoof SIP headers so they don’t match the corresponding UDP headers

2.2 TRANSPORT LAYER

The transport Layer (Layer 4 in the OSI model) is especially vulnerable for the Denial of Service (DOS) attack or Distributed Denial of Service (DDOS) attack. Two most popular protocols used in the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). The following are the key security risks at the Transport Layer associated with TCP and UDP:

TCP SYN Attack

It is also known as SYN Flooding. It takes advantage of a flaw in how most hosts implement the TCP three-way handshake. When Host B receives the SYN request from A, it must keep track of the partially opened connection in a "listen queue" for at least 75 seconds. Many implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN&ACK the other host sends back. By doing so, the other host's listen queue is quickly filled up, and it will stop accepting new connections, until a partially opened connection in the queue is completed or times out. This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack, or it can be used as a tool to implement other attacks, like IP Spoofing..

SSL Man-in-the-Middle Attacks

SSL/TLS was supposed to mitigate that risk for web transactions by providing endpoint authentication and encryption. However, it is discovered in late 2000 the feasibility of mounting an MITM attack on the protocol. One faulty SSL client Implementation, Microsoft's Internet Explorer, allows for transparent SSL MITM attacks when the attacker has any CA-signed certificate. An even greater risk is posed by unprotected systems where an attacker can preload his/her own trusted root authority certificates. The mitigation for such attack is to properly configure client SSL that would warn the user about problems with the server certificate.

Land Attack

An attacker sends a forged stream of TCP SYN packets with the same source and destination IP address and TCP port numbers. The victim system will be confused and crashed or rebooted. Service providers can block LAND attacks that originate behind aggregation points by installing filters on the ingress ports of their edge routers to check the source IP addresses of all incoming packets. If the address is within the range of advertised prefixes, the packet is forwarded; otherwise it is dropped.

TCP Connecting Hijacking

It is also known as Man-in-the-Middle attack. With this attack, an attacker can allow normal authentication to proceed between the two hosts, and then seize control of the connection. There are two possible ways to do this: one is during the TCP three-way handshake, and the other is in the middle of an established connection. Connection hijacking exploits a "desynchronized state" in TCP communication. When two hosts are desynchronized enough, they will discard (ignore) packets from each other. An attacker can then inject forged packets with the correct sequence numbers (and potentially modify or add commands to the communication). This requires the attacker to be located on the communication path between the two hosts so that he may eavesdrop, in order to replicate packets being sent.

UDP Flood Attack

UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

Port Scan Attack

A Port Scan is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a network run many services that use TCP or UDP ports. A port scan helps the attacker find which ports are available. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

3 PRECAUTIONS TO AVOID ATTACK

BE AWARE OF

a) Anti Virus Software, Firewalls

Start with the basics. Basic Internet security protection is the first line of defense against DDoS attacks. Firewalls, anti-virus and anti-malware programs give your PC some ability to block crude or "brute force" DDoS attacks. Make sure all of your software and OS installs are updated and run an anti-malware program on a regular basis.

b) Protect your mail servers

One method of DDoS attack targets the mail servers of large organizations. The scale of the mail servers make the servers vulnerable to DDoS attacks. Use a mail server software that provides explicit protection against DDoS attacks.

c) Work with your web host

If you think that you might become the target of a DDoS attack or are currently being attacked, contact your web host (if you're running a website) or your Internet service provider and ask the company to investigate. The web host or ISP can block the range of IP addresses that are taking part in the attack, thereby blocking all or part of the attack.

d) RATs (Trojan Horse Program)

RATs are more dangerous than all other types of malicious code. To protect yourself, become familiar with the types of RATs, how they work, and how to detect and prevent these pests.

RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs such as Symantec's pc Anywhere but are designed specifically for stealth installation and operation. Intruders usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs. Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email attachments.

4 CONCLUSION

Like most of the network security problems, there are no silver bullet solution to fix the problems, however, there are many technologies and solutions available to mitigate the above security problems and to monitor the network to reduce its damage if attack occurs but we should be aware of the precaution to avoid these DDoS attacks.

REFERENCES

[1] Distributed Denial of Service:Taxonomies of Attacks, Tools and Countermeasures Stephen M. Specht Electrical Engineering Princeton University Princeton, NJ 08544 stephen.specht@us.army.mil Ruby B. Lee Electrical Engineering Princeton University Princeton, NJ 08544 rblee@princeton.edu

[2] A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment. This paper is from the SANS Institute Reading Room site

[3] Attacks on layer two of the OSI model by David Barroso and Alfredo Andres.

[4] Managing the Threat of Denial-of-Service Attacks. Allen Householder, CERT/CC,Art Manion, CERT/CC,Linda Pesante, CERT/CC,George M. Weaver, CERT/CC,In collaboration with:Rob Thomas.

[5] Detecting Distributed Denial of Service ttacks Using Source IP Address Monitoring.Tao Peng Christopher Leckie Kotagiri Ramamohanarao.

[6] Denial of Service and Distributed Denial of Service on the Internet. K. Ormiston and MM Eloff Business Connexion, School of Computing, UNISA kate.ormiston@bcx.co.za, eloffmm@unisa.ac.za