International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

An Analysis of TCP SYN Flooding Attack and Defense Mechanism

Manish Kumar, Arvind Panwar, Achin Jain
M. Tech. (IS) AIACTR, Geeta Colony, New Delhi

ABSTRACT

The SYN flooding attack is frequent network based Denial of Service attack. This attack exploits the vulnerability of TCP connection known as 3 way handshaking. The SYN flooding attack sends too TCP SYN request to handle by the server. This action causes victim system responds slowly.

The paper contributes a detailed analysis of the SYN Flooding attack and a discussion of existing defense mechanism.

1. INTRODUCTION

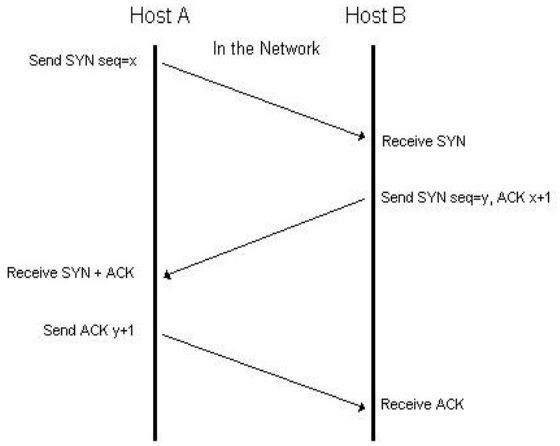
Since September 1996, several dozen sites on the Internet have been subjected to a denial of service attack, popularly called *SYN Flooding*. A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. It has been shown that more than 90% of the DoS attacks use TCP. Recent experiment have shown that a specialized firewall, which is designed to resist SYN floods, became futile under a flood of 14,000 packets per second[1].The TCP SYN flooding is the most commonly-used attack. It consists of a stream of spoofed TCP SYN packets directed to a listening TCP port of the victim. Not only the Web servers but also any systems connected to the Internet providing TCP-based network services, such as FTP servers or Mail servers, are susceptible to the TCP SYN flooding attacks.

2. THE SYN FLOODING ATACK

Normally when a client attempts to start a TCP connection (Figure 3) to a server, the client and server exchange a series of messages which normally runs like this:

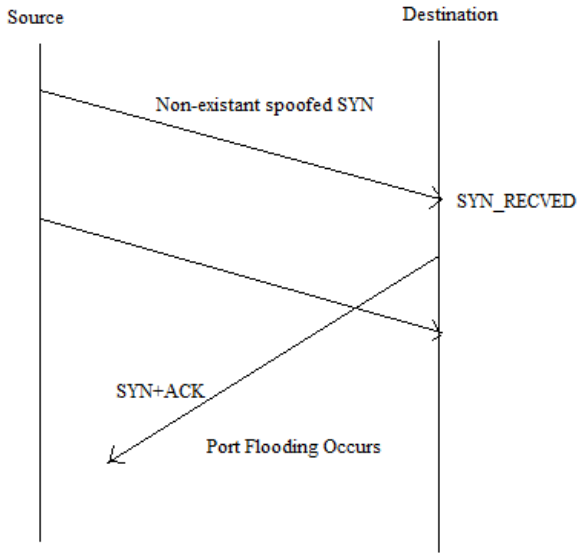
1. The client requests a connection by sending a SYN (*synchronize*) message to the server.
2. The server *acknowledges* this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established [10].

Fig 1. Normal TCP Connection (3-way Handshake)



Until the SYN/ ACK packet is responded by the client connection remains in half open state for up to 75 seconds. For all the half open connections, server maintains a backlog queue. The backlog queue is of finite size. When the queue is full then all new connection request is dropped. Consider when SYN packet is spoofed then server never receives the SYN/ACK packet by client. Hence flooding of such SYN packets can easily exhaust the victim server's backlog queue and all new incoming SYN packets can be dropped. However the existing connection is not affected.

Fig 2. A System under Attack [2]



.

The major attention of the attacker requires the source IP address which is used to establish a connection to a victim machine. Attacker chooses the IP address which is not reachable. If the source IP address is reachable then the host will receive SYN+ACK from the victim server without having requested a connection. In this case the source will send a RST packet to server that cause server to reset the connection.

It is therefore in the interest of an attacker to forge source addresses that do not belong to hosts that are reachable from the victim server. The goal of the TCP SYN flooding attack is depleting the backlog which attempts to send enough SYN segments to fill the entire backlog. The amount of CPU and network bandwidth required by an attacker for a sustained attack is negligible.

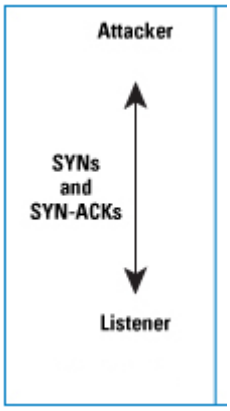
3. Methods of Attack

The attack can be categorized on the basis of observation on the internet: Direct Attack, Spoofing-Based Attack and Distributed Attack [9].

3.1 Direct Attack

In this type of attack, the attacker rapidly sends SYN segments without spoofing their IP address. To do this effectively, a user must prevent his/her operating system responding to the SYN+ACK in any way to prevent sending RST packet against each SYN+ACK packet. Attackers can do this by changing the rule of the firewall. Figure (3) shows this attack.

Figure (3). Direct Attack [9]



This attack is very easy to defend by defining the rule on firewall to block blocker's IP address.

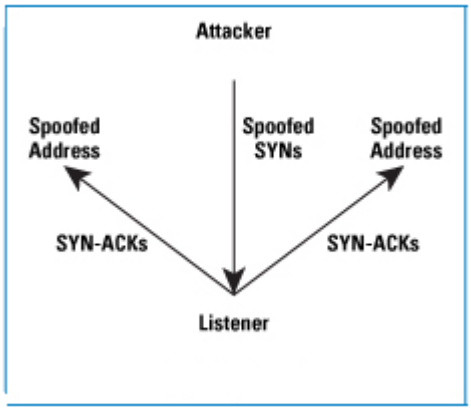
3.2 Spoofed-based Attack

In this type of attack attacker attacks on the victim machine by set of spoofed IP address shown in figure (4). For spoofing attack, a primary consideration is address selection [9]. An attacker can choose spoofed IP address by two ways:

A) **Single Source**: - An attacker can use single source address which will not respond to SYN+ACK by any machine. The chosen IP address either does not exist or can't be figure out due to some property of address or network configuration.

B) **Short list**:-In another approach the attacker use a list of different source addresses under the assumption that some percentage of spoofed address will not be responded by victim machine. This makes defense more difficult.

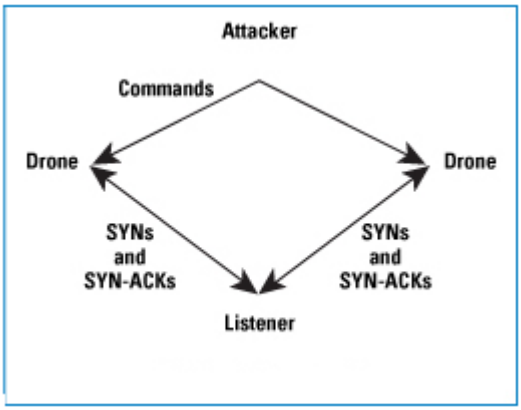
Figure(4) Spoofed-based Attack [9]



3.3 Distributed Attack

This version of SYN flooding attack the attacker attacks by the numerous drone machines throughout the internet (figure 5). This attack is much more difficult to counter.

Figure 5. Distributed Attack [9]



The drone machines are constantly added or removed from the attack list and also can change their IP addresses therefore it is quite difficult to block these attacks.

4. DEFENSE MECHANISM

4.1 SYN Cache

SYN caching allocates some state on the machine, but even with this reduced state it is possible to encounter resource exhaustion. The code must be prepared to handle state overflows and choose which items to drop in order to preserve fairness. The initial SYN request carries a collection of options which apply the TCP connection; these commonly include the desired message segment size, requested window scaling for the connection, use of timestamps, and various other items. Part of the purpose of the allocated state is to record these options, which are not retransmitted in the return ACK from the client [3].

4.2 SYN Cookies

SYN cookies do not store any state on the machine, but keeps all state regarding the initial TCP connection in the network, treating it as an infinitely deep queue [3].

4.3 Hybrid Approach

This is the mechanism to combine any two or more than two defense mechanisms. For example if we combine large backlog and SYN cookies then it will be more robust than individual mechanism [9].

4.4 Reduce the SYN-RECEIVED Time

To defend against the exhaustion of resources in the systems under attack, an obvious approach is to increase the number of resources devoted to half-open TCP connections, and to reduce the timeouts.

These measures have been suggested by different sources [6], and can be summarized as:

1. Reduce the timeout period from the default to a short time,
2. Significantly increase the length of the backlog queue from the default (see Table 2).
3. Disable non-essential services, thus reducing the number of ports that can be attacked [2].

Table 1 .Backlogs for some operating System [2]

Operating System	Backlog	Backlog +Grace
FreeBSD 2.1.5	n.a.	128
Linux 1.2.x	10	10
Solaris 2.4	5	n.a.
Solaris 2.5.1	32	n.a.
SunOS 4.x	5	8
Windows NTs 3.51	6	6
Windows NTw 4.0	6	6

4.5 Filtering

The measures proposed in the first reactions to the recent attacks [7], as well as several other sources [8] attempt to make it difficult for packets with spoofed source addresses to traverse routers. The solutions proposed can be summarized as follows:

1. Configure external interfaces on routers to block packets that have source addresses from the internal network.
2. Configure internal router interfaces to block packets to the outside that have source addresses from outside the internal network [2].

4.6 Firewall Approach

Most of the site today is protected by the firewalls, hence to protect against SYN flooding attack firewall can be a very useful tool. Several firewall vendors have already made products available to increase protection against the attacks [4, 5], and some other solutions have been proposed.

Firewall-based protection approaches are based on the idea that every packet destined to a host inside the firewall has to be examined by the firewall first, and thus decisions can be made on its authenticity and actions can be taken to protect the internal hosts [2].

4.6.1 Firewall as a Relay

In this approach, when a packet for an internal host is received the firewall answers on its behalf. Only after the three-way handshake is successfully completed does the firewall contact the host and establish a second connection [2].

4.6.2 Firewall as a Semi-transparent Gateway

In this approach, the firewall lets SYN and ACK packets go through, but monitors the traffic and reacts to it. The firewall passes SYN packets destined to internal hosts. When the host responds with a SYN+ACK packet, the firewall forwards it, but reacts by generating and sending an ACK. packet that seems to come from the client [2].

4.7 Active Monitoring

This category of solutions consists of using software agents to continuously monitor TCP/IP traffic in a network at a given place. An agent can collect communication control information to generate a view of all connections that can be observed on a monitored network. Furthermore, it can watch for certain conditions to arise and react appropriately [2].

The above mentioned mechanism can be classified into two broad classes on the basis of where the defenses are implemented [9].

1) End Host Mechanism

This involves hardening the end host TCP implementation itself, including altering the

algorithms and data structures used for connection lookup and establishment, as well as some solutions that diverge from the TCP state machine behavior during connection establishment [9].

2) Network based Mechanism

This category of mechanism involves hardening the network, either to lessen the likelihood of the attack preconditions (an army of controlled hosts or the propagation of IP packets with spoofed source addresses), or to insert middle boxes that can isolate servers on the networks behind them from illegitimate SYNs [9].

Both end-host and network-based solution has merits and demerits. Both types of attack is used frequently. The table 1 gives some idea about the performance of the above mentioned attack mechanisms.

Table 1. Comparative analysis of defense mechanisms.

Mechanism category	Defense Mechanism	Performance
Network Based	Filtering	This is highly effective to prevent SYN flooding attack but not currently reliable due to non implementation universally.
	Firewall	This performs very well but it may disable some high performance because it splits the TCP connection.
	Active Member	Cheaper to implement and good option to protect entire network without involving the listener's operating system.
End Host	Increasing TCP backlog	Could be relied upon because an attacker can generate attack segments which are able to scale any backlog supported by a host.
	Reduce the SYN-RECEIVED Time	Imposes some amount of congestion which cause the lost of legitimate ACK packets.
	SYN Cache	This is the best end host mechanism available and able to establish legitimate connection with in 15% increase in latency [3].
	SYN Cookies	Does not possess any state, very effective even under heavy attack but it cause to degrade the performance [9].
	Hybrid	Combination of different defense mechanisms and very strong to protect the attack.

CONCLUSION

As the no of internet user increased exponentially the no of attacks also increased. Among all the attacks SYN Flooding attack is more in the news of network security domain. This paper described the SYN flooding attack, the types of attack and their countermeasure. We also analyzed and categorized the defense mechanism to make the attack ineffective. Finally we presented a comparative performance analysis on these mechanisms.

REFERENCES

1. Haining Wang, et al., "Detecting SYN Flooding Attack", International Conference on Distributed Computing Systems, Jul. 2002

2. Christoph L. Schuba et al, "Analysis of a Denial of Service Attack on TCP" in proceeding IEEE 1997

3. J. Lemon, "Resisting SYN Flooding DoS Attacks with a SYN Cache",*Proceedings of USENIX BSDCon'2002*, February, 2002

4. L. S. Laboratories. Livermore SoftwareLubs. Announces Defense agains SYN Flooding Attacks, October 1996.

5. C. P. S. T. Ltd. TCP SYN Flooding Attack and the Firewall- 1 SYNDefender, October 1996.

6. M. Graff. *Sun Security Bulletin 00136.* Mountain View, CA, Oct. 1996.

7. Computer Emergency Response Team (CERT), Camegie Mellon University, Pittsburgh, PA. *TCP SYN Flooding and IP Spoofing Attacks,* Sept. 1996. CA-96:21.

8. Cisco Systems Inc. *Defining Strategies to Protect Against TCP SYN Denial of Service Attacks,* September 1996.

9. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html

10. http://en.wikipedia.org/wiki/SYN_flood