A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations

Deepak Singh Rana
Dept. of Computer Application
Graphic Era University
Dehradun, India
deepakranageu@gmail.com

Naveen Garg
Dept .of Computer Science and
Engg. Graphic Era University
Dehradun, India
na_garg@rediffmail.com

Sushil Kumar Chamoli
Dept. of Computer Application
Graphic Era University
Dehradun, India
sushilchamoli@gmail.com

Abstract

Flooding attacks are major threats on TCP/IP protocol suite these days; Maximum attacks are launched through TCP and exploit the resources and bandwidth of the machine. Flooding attacks are DDOS (Distributed denial of service) attacks and utilize the weakness of the network protocols. SYN flood exploits the 3-way handshaking of the TCP by sending many SYN request with IP spoofing technique to victim host and exhaust the backlog queue resource of the TCP and deny legitimate user to connect. Capturing the packet flow is very important to detecting the DOS attack. This paper present how the TCP SYN flood takes place and show the number of packets received by the victim server under the attack.

Keywords—SYN FLOOD, TCP, DDOS

1. Introduction

In rapid growth of Internet security is measure issue in networks. The internet presently carries an huge amount of undesirable network communication. Most of the network traffic is controlled by Transport Control Protocol [1] these days .The traffic control and its management is the crucial factor for smooth running of networks. TCP SYN flood attack is one of the distributed denials of service attack, has been widely observed worldwide and occupies about 80 to 90 % source of DDOS attacks. TCP SYN flood attacks typically target different websites, web-servers of large organizations like banks, credit card, payment gateways, and even name **servers.** In TCP SYN flood attack, attackers send TCP connection request faster than a computer can process them, it sends large number of SYN packets (request) with IP spoofing techniques to the victim host and exhaust the TCP connection queue. The victim server receive the SYN packet and send SYN +ACK to client but never receive ACK packet, this accessing the regular services. In this paper we detect the SYN flood attack on a host in network.

We capture packets using network monitoring tool wire-shark software and recording of the TCP packets are done. Because DDOS attacks are distributed and use botnets to launch the attack , it is quiet easy to find the attack from the single attacker if IP address used is original, by counting the SYN packets send by the attacker but is difficult when attackers use spoofed IP addresses .

2. TCP Three Way Handshaking

TCP is stream, connection oriented protocol for packet network Intercommunication, developed by Vinton G.Cerf and Robert K.khan . TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. The data/messages are broken by TCP into segments and each segment consist a specific format [1]. TCP use full duplex service in which data can flow in the both directions, use three way handshaking to establish connection.

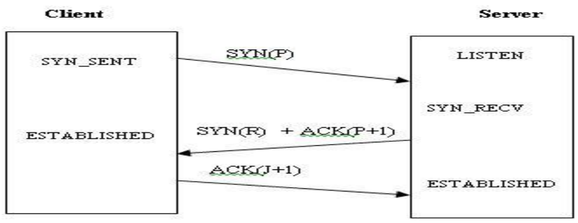


Figure 1.TCP 3 Way Handshaking

In connection establishment process, firstly the client sends the first segment a, SYN segment to server, after receiving SYN segment from client server sends a

SYN+ACK segment back to client and then client responds with ACK segment and the connection is established.

A. *Active Connection in TCP*

A client process using TCP takes the “active role” and initiates the connection by actually sending a SYN message to start the connection [8].

B. *Passive connection in TCP*

Passive Open connection [8] is used by TCP when running a server application, for example a Web Server. The TCP socket opens in passive mode and waits for incoming connections.

C. *Half open Connection in TCP*

An connection is said to be "half-open" if one of the TCP has closed or aborted the connection at its end without the knowledge of the other side [7] .

3. IP Spoofing

IP spoofing is the creation of IP packets using forged IP source addresses. It is used for the purpose of concealing the identity of the sender. IP spoofing is most frequently used in denial of service attack. In such attacks, the goal of attackers is to flood the packets with overwhelming amount of traffic, and the attacker does not care about receiving response back to the IP packet. IP spoofing use randomized IP addresses and become the source address of the attacks. Spoofed IP addresses are difficult to filter since each spoofed packet appears to come from a different address, and in this way they hide the true source of the attack.

4. TCP SYN Flood Attack

TCP SYN flood attack is distributed denials of service attack (DDOS) in which attackers send large number of spoofed packets to a server and exhaust the resources of the server and deny legitimate user to connect.

Commonly used SYN flooding attacks leverages on TCP’s state retention on establishing a new connection on server. TCP SYN flooding attacks exploit the standard TCP three way handshake, in which the server receives a client’s SYN request, replies with a SYN+ACK packet and than wait for the client to send the ACK to complete the handshaking, while waiting the ACK from client machine server maintain a half open connection. Because attackers chooses spoofed IP addresses as its source addresses of the attacking packet, server will not receive the final ACK from client never, in this way large number of half open connections are maintained on a victim server’s queue and it get full. The queue of the server is limited, and legitimate client’s request can not be fulfil due to unavailability of the resources (space) in the queue.

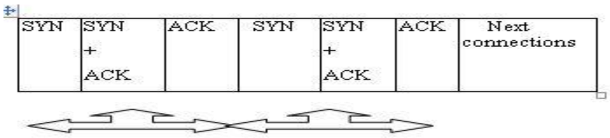


Figure2. Status of Queue in three way handshaking without attacks.

A successful connection establishment is shown in figure1, and the connection queue in figure 2, where SYN and ACK are transferred between the client and server.

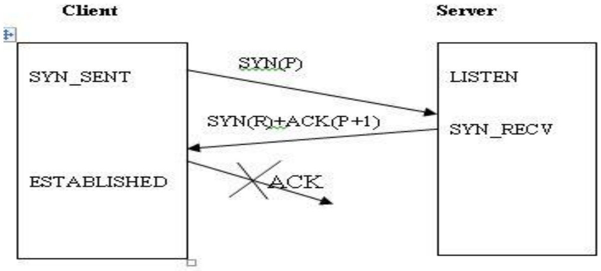


Figure3. TCP 3 Way Handshaking with no ACK from client

A connection is half open state shown in figure 3 where client sends SYN to server ,Server sends SYN+ACK back to client assuming that client exist but server never get back the ACK (acknowledgement) from client and goes to the half open state. While the request is waiting to be confirmed from client, it remains in the server queue. Each half-open connection will remain in the memory queue until it times out, it will retransmit the SYN+ACK 5, doubling the timed out value after each retransmission. The first value is 3 seconds for retransmission, are attempted at 6,12,24,48 seconds respectively. SYN floods can be launched from compromised machines original and spoofed source IP addresses.

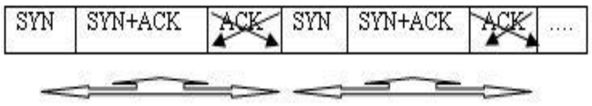


Figure 4. Status of Queue with SYN flood attacks

5. Related Works

TCP probing for reply Argument Packet [4] is the methods used for the mitigation of TCP SYN flood with IP spoofing. The sender of spoofing packets mostly unable to see any replies with this in the mind, TCP Probing for reply Acknowledgment Packet which intelligently craft/append TCP acknowledgement messages to give another layer of protection.In this method extra specification is appended with the acknowledgement that is to change the TCP window size or cause packet retransmission.

To mitigate the SYN flooding attack SYN cookies [5] is used SYN cookies work to alleviate SYN floods by calculating cookies that are functions of the source address, source port, destination address, destination port and random secret seed. On receiving SYN packet the server calculates a SYN cookie and sends it back to client as part of the SYN+ACK and do not allocate resources for the request send by client. when ACK packet is received the connection is established if a valid cookie is present in the ACK packet.

SYN cache also used to mitigate the flooding attacks, It use the concept of backlog queue, a minimum amount of state is stored for each SYN request.

Hop-Count Filtering [3] uses the hop count of packets arriving at a particular server. This method maps IP address to hop counts, in case of spoofed packet hop count of the respected packet will not match the expected hop count. HCF only filter traffic if some threshold amount of packets does not match their expected hop counts.

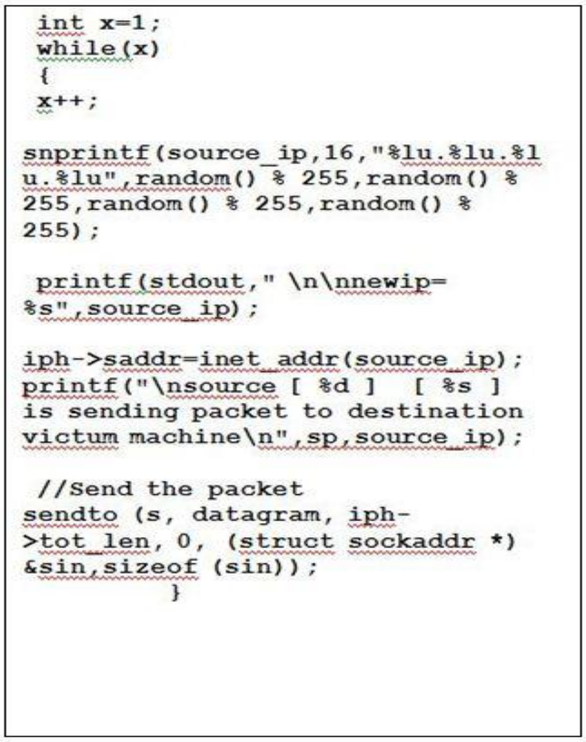
A way to mitigate IP-spoofing IP puzzles [2] are used ,it provides active defence against IP-spoofing, in which server sends a IP puzzle to the client ,now client need to solve the puzzle, if solution by client is correct ,then only server allow to connect and start the data ransfer.

Modern operating system comes with the sufficient backlog queue ,the size of backlog queue can be increased as per requirements . Increasing the backlog queue simply creates more resources for the server to accommodate more TCP request in half open state .

6. Packet Generation for TCP SYN flooding

In order to detect the TCP SYN flood attack on the victim server, we use a 'C' program based on Linux socket to send the large number of packets.to server. C functions that can be used to program communications, residing on different computer, connected with TCP/IP network.

When 'C' script executed from a client machine it sends SYN packets to server with spoofed IP addresses ,network bandwidth of server is consumed due to handle these request from spoofed IP addresses .



```
 int x=1;
 while(x)
 {
 x++;

snprintf(source_ip,16,"%lu.%lu.%l
u.%lu",random() % 255,random() %
255,random() % 255,random() %
255);

 printf(stdout," \n\nnewip=
%s",source_ip);

iph->saddr=inet_addr(source_ip);
printf("\nsource [ %d ]   [ %s ]
is sending packet to destination
victum machine\n",sp,source_ip);

 //Send the packet
sendto (s, datagram, iph-
>tot_len, 0, (struct sockaddr *)
&sin,sizeof (sin));
           }
```

Figure 5. 'C' code for SYN flood

Here random function is used to generate a new IP address every time, by which SYN packet seems to be coming from different sources.

Sendo function used for send the syn packet to the server.

7. Packet capturing

The packets are captured using Wireshark [9], which is a network packet capturer in Linux and windows environment. A packet capturer, like Wireshark allows us to capture and display network packets details. In this paper we Wireshark is used to ascertain that our packet generator (the C script) generates SYN packets, to collect statistics on the SYN packets processed by the victim server , monitor TCP service request sent by the different client machines .

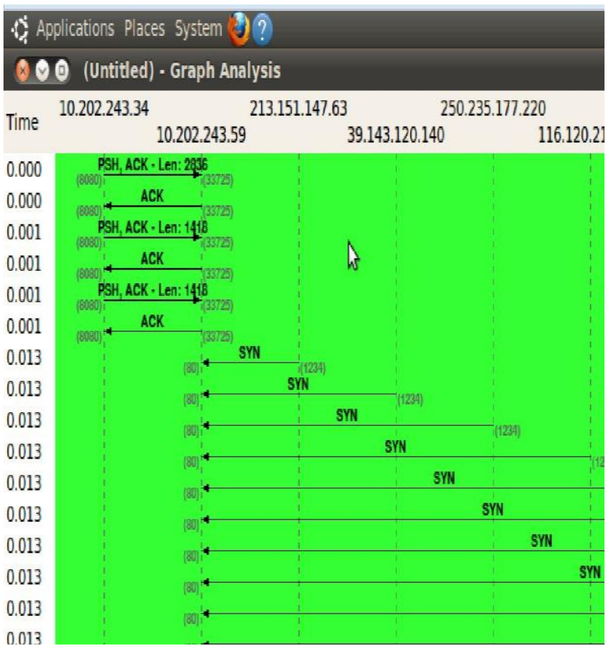


Figure6. SYN packets received on victim server.

Figure 6 shows only SYN packets are received at the server end from different IP addresses with one second time interval.

8. Detection of SYN flood on Host

SYN flood attack can be detected by monitoring the TCP states, netstat is the command both in Linux and Windows environment used to display the status of network connections in the host.

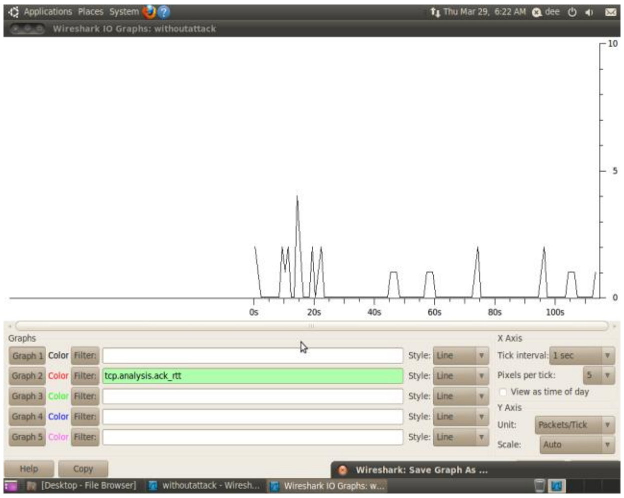
The half open connections in Linux is encoded as SYN_RECV state only.

```
$netstat –n –p –t | grep SYN_RECV |wc –l
```

Above command can count the number of half open connections in a system at that instant .

9. Number of Packets captured at victim machine with no attack

Figure 7 shows the number of packets on a machine captured by wireshark, we filter packets by tcp.analysis.ack_rtt , result shows maximum 5 to 10 packets are captured at the network interface of the server machine.


Applications Places System
Thu Mar 29, 6:22 AM dee
Wireshark IO Graphs: withoutattack
10
5
0
0s
20s
40s
60s
80s
100s
Help
Copy
Wireshark: Save Graph As ...
[Desktop - File Browser]
withoutattack - Wiresh...
Wireshark IO Graphs: w...

Graphs

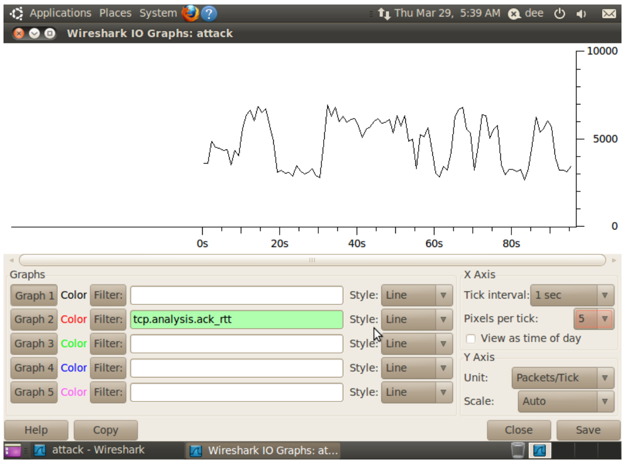
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: tcp.analysis.ack_rtt Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto

Figure7.Total number of packets per second received on victim server with no attack.

10.Number of Packets captured at victim machine with SYN flood attack

Figure 8 shows the number of packets on a victim server captured by Wireshark, we filter packets by tcp.analysis.ack_rtt , result shows 2000 to 7000 packets are captured at the network interface of the server machine. In this way SYN flood attack consume the network bandwidth and resources on the victim machine.



Filter: tcp.analysis.ack_rtt
Style: Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto

Figure8.Total number of packets per second received on victim server with SYN flood attack.

11. TCP SYN flooding mitigations

***A* . TCP probing for reply Argument Packet** [4] is the methods used for the mitigation of TCP SYN flood with IP spoofing. The sender of spoofing packets mostly unable to see any replies with this in the mind, TCP Probing for reply Acknowledgment Packet which intelligently craft/append TCP acknowledgement messages to give another layer of protection. In this method extra specification is appended with the acknowledgement that is to change the TCP window size or cause packet retransmission.

In this method server sends SYN+ACK+craft message to client back , the result from the learning /recording packet analyzer ,checks whether the TCP reply acknowledgement packet satisfies the specification given by the server using TCP probing to change the TCP window size.

B. Increase the Backlog queue of the server

In This method we simply increase the backlog queue of the server to maintain more half open connections, tcp_max_syn_backlog is the parameter to set in the mostly Linux operating system.

C .SYN cookies

To mitigate the SYN flooding attack SYN cookies [5] is used SYN cookies work to alleviate SYN floods by calculating cookies that are functions of the source address, source port, destination address, destination port and random secret seed. On receiving SYN packet the server calculates a SYN cookie and sends it back to client as part of the SYN+ACK and do not allocate resources for the request send by client. when ACK packet is received the connection is established if a valid cookie is present in the ACK packet. The TCP parameter tcp_syncookies in Linux is directly involved in mitigation of SYN flood attack [11].

12. Conclusion and future work

In this paper we successfully provided a simple experiment to produce a TCP SYN flooding DDOS attack, we estimate the packet rate on a victim server per second. In future we like to analyze and provide solutions to other flooding attacks on network like UDP flooding etc, both in wired and wireless.

13. References

[1] J. Postel ,"Transmission Control Protocol",RFC793,9/81

[2] Ma, M, "Mitigating denial of service attacks with password puzzles" in Information Technology: Coding and Computing, Vol. 2, May 2005. pp.62 1 - 626.

[3] Bharathi KrishnaKumar, P.Krishna Kumar "Hop Count Based Packet Processing Approach to Counter DDoS Attacks" International Conference on Recent Trends in Information, Telecommunication and Computing, 2010

[4] L .Kavisankar , C. Chellapan ," A Mitigation model for TCP SYN flooding with IP Spoofing", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 , pp. 251-256.

[5] D.J. Bernstein, "SYN Cookies" 1997 [online] , http://cr.yp.to/syncookies.html

[6] Stopforth, Riaan: Techniques and countermeasures of TCP/IP OS fingerprinting on Linux Systems, Thesis, University of KwaZulu-Natal, Durban, 2007

[7] TCP SYN flooding and common mitigation RFC

[8] http://www.tcpipguide.com/free/t_TCPConnectionPreparation TransmissionControlBlocksT-2.htm

[9] Wireshark, www.wireshark.org

[10] http://www.frozentux.net/ipsysctl-tutorial/chunkyhtml/tcpvariables.html

[11] D. Kirkland, TCP protocol ,http://manpages.ubuntu.com/manpages/aunty/man7/tcp.html