International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Analysis of Sync Flood Attack on Web Servers

[1]Amadi E.C., [2]Ugo C. C., [3]Ezughalu E. E., [4]Maduako C.

[1-4]Department of Information Management Technology, Federal university of Technology, Owerri, Imo State, Nigeria

ec.amadi@gmail.com

Abstract

Floodingattacksaremajorthreatson TCP/IP protocol suite these days; Maximum attacks are launched throughTCPandexploittheresourcesandbandwidth of the machine. Flooding attacksare DDOSattacksandutilize the weaknessofthe networkprotocols.SYNfloodexploits the3-wayhandshakingoftheTCPbysendingmany SYNrequestwithIP spoofingtechniquetovictimhost and exhaustthebacklogqueueresourceoftheTCP anddeny legitimateusertoconnect. Capturing the packet flow is very important to detecting the DOS attack. This paperpresentsa review of how the TCPSYN flood takesplace and its devastating effect on webservers on the internet.

Keywords—SynFlood,Tcp/Ip,Ddos, Bandwidth, Protocol

1. Introduction

Postel, (1999) Inrapidgrowthofinternetsecurity ismeasureissuein networks. The internet presently carries a huge amountofundesirablenetworkcommunication.Mostof the network traffic is controlled by TransmissionControlProtocolthesedays. The trafficcontroland itsmanagementisthe crucialfactorfor smoothrunning of networks.J.Postel, (1999) TCPSYNfloodattackisone of the distributeddenialsof serviceattack,hasbeenwidely observed worldwideandoccupiesabout80%to90% sourceof DDOSattacks.TCPSYNfloodattacks typically targetdifferentwebsites,web-servers oflarge organizations like banks, creditcard,payment gateways,andevennameservers.InTCPSYN flood attack, attackers send TCP connection request faster than a computer can process them, it sends large numberof SYNpackets(request)withIPspoofing techniques to the victimhost and exhaust the TCP connectionqueue.Thevictim server receivethe SYN packetandsendSYN+ACK (acknowledgement) toclientbutneverreceive ACKpacket.Inthis paper, wedetect theSYNflood attack on ahostin network.

Postel, (1999) Wecapture packets using network monitoring tool wire-sharksoftwareandrecording oftheTCPpackets aredone.BecauseDDOSattacksaredistributedand usebotnetstolaunchtheattack,itisquieteasy tofind theattackfrom thesingleattackerifIPaddressusedis

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

original,by counting theSYNpacketssendby the attackerbutisdifficultwhenattackersuse spoofedIP addresses.

2.TCPThreeWayHandshaking

Postel, (1999) TCPisstream,connectionorientedprotocolfor packet networkIntercommunication,developedby Vinton G.CerfandRobertK.khan. Kavisankar,&Chellapan (2011) TCPallowsthesending processtodeliverdataasa stream ofbytesandallows the receiving process to obtain data asastreamof bytes.Thedata/messagesare brokenbyTCPinto segmentsandeachsegmentconsists of aspecificformat. TCPusefullduplexserviceinwhichdatacan flowinthebothdirections,usethreewayhandshaking toestablishconnection.

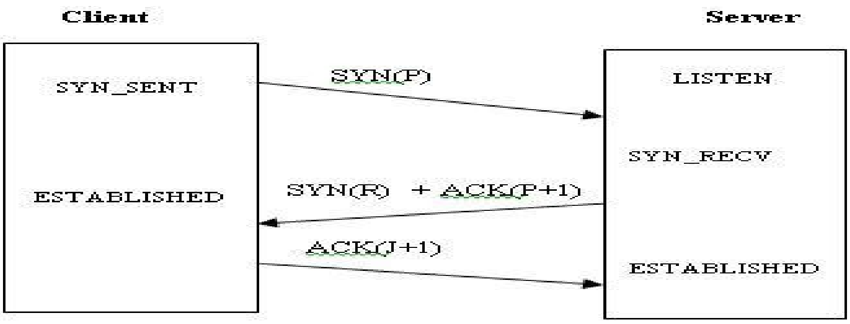

Figure 1.TCP3 Way Handshaking, (Kavisankar, and Chellapan, 2011P. 151)

Inconnectionestablishmentprocess,firstly theclient sendsthe firstsegment,a SYN segmenttoserver.After receiving SYN segment fromclient, server sends a SYN+ACK segmentbacktoclientandthenclient respondswithACK segmentandtheconnectionis established.

a. ActiveConnectioninTCP
A clientprocessusingTCPtakesthe**activerole**and initiatestheconnectionby actuallysendingaSYN message to starttheconnection.

b. PassiveconnectioninTCP
PassiveOpenconnectionisusedby TCPwhen running aserverapplication, for examplea Web Server. The TCPsocketopensinpassivemodeand waitsforincomingconnections.

c. HalfopenConnectioninTCP
Aconnectionissaidtobe"half-open" ifone ofthe TCPhasclosedorabortedtheconnectionatits end withouttheknowledgeoftheotherside.

.3. IPSpoofing

IPspoofingisthecreationofIPpacketsusingforgedIP source addresses. It is used for the purpose of concealingtheidentityofthesender. IPspoofingis mostfrequentlyused indenialofservice attack.In

International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

such attacks,thegoalofattackersistoflood thepacketswith overwhelming amountof traffic,andtheattackerdoes notcareaboutreceivingresponsebackto theIPpacket. IPspoofinguserandomizedIPaddressesandbecome the sourceaddressoftheattacks.SpoofedIPaddresses aredifficulttofiltersinceeachspoofedpacketappears tocomefrom adifferentaddress,andinthiswaythey hidethetruesourceoftheattack. (Postel, 1999)

4. TCPSYNFloodAttack

Bernstein (2007) explains that “TCPSYNfloodattackisdistributeddenialsof service attack(DDOS)inwhichattackerssend largenumberof spoofedpacketsto a serverandexhausttheresources oftheserver anddenylegitimateusertoconnect”(Bernstein, 2007, p.150).

(Kavisankar,Chellapan, 2011) explains that “Commonlyused SYNfloodingattacksleverages on TCP’sstateretentiononestablishinganew connection on server. TCP SYN flooding attacks exploit the standardTCPthreeway handshake,inwhichtheserver receivesa client’s SYNrequest,replieswitha SYN+ACK packetandthenwaitfortheclienttosend theACKtocompletethehandshaking,whilewaiting for theACKfromclient,machineserver maintainahalf openconnection” (Kavisankar&Chellapan, 2011, p.120). Becauseattackerschoosesspoofed IPaddressesasitssourceaddressesof the attacking packet, server will not receive the final ACKfrom client never, in this waylarge numberofhalfopen connectionsaremaintainedonavictim server’squeue anditgetfull.The queue of the serverislimited,and legitimateclient’s requestcannot befulfilldueto unavailabilityofthe resources(space) in thequeue.

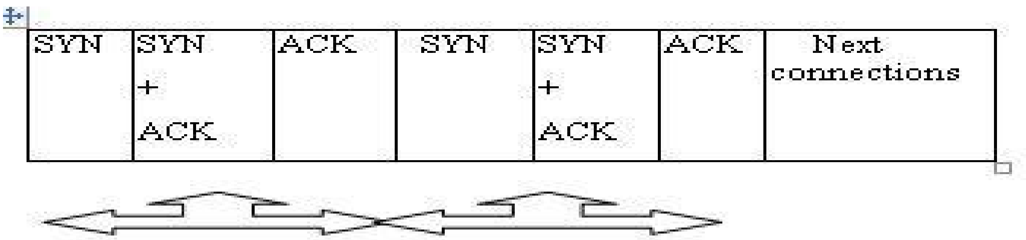

Figure 2.Status ofQueueinthreewayhandshaking withoutattacks.(Kavisankar,and Chellapan, 2011P. 151)

A successfulconnectionestablishmentisshownin figure1,andtheconnectionqueue infigure2,where SYNandACK aretransferredbetweentheclientand server.

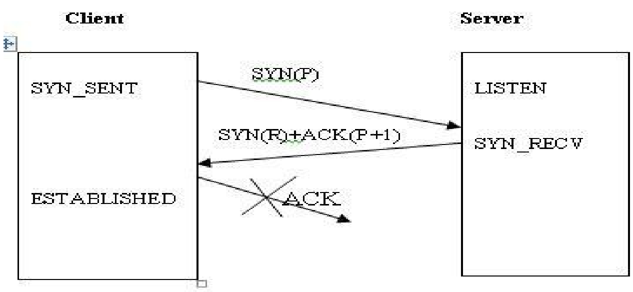

Figure3. TCP 3 Way Handshaking withno ACK fromClient (Kavisankar, and Chellapan, 2011)

Bharathi et al (2010) explains that "Aconnectionishalfopen state shown infigure3where clientsendsSYN toserver, ServersendsSYN+ACK back to client assuming that client exist but server never get backthe ACK (acknowledgement) fromclientandgoestothehalfopenstate.Whiletherequest iswaitingtobeconfirmedfromclient,itremainsinthe serverqueue" (Bharathi et al 2010, p.100).

Eachhalf-openconnectionwillremainin thememoryqueueuntilittimesout,itwill retransmit theSYN+ACK5,doublingthetimedoutvalueafter eachretransmission.Thefirst valueis3secondsfor retransmission,are attemptedat6,12,24,48 seconds respectively. SYN floods can be launched fromcompromisedmachinesoriginaland spoofed sourceIP addresses.

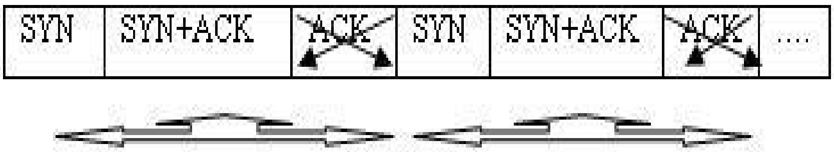

Figure 4.StatusofQueuewithSYNfloodattacks (Kavisankar, and Chellapan, 2011)

5. RelatedWorks

Kavisankar, and Chellapan, (2011) states that "TCPprobing forreplyArgumentPacketisthe methods used forthemitigation ofTCPSYNflood with IP spoofing" (Kavisankar&Chellapan, 2011, p.98). The sender of spoofing packets mostly unabletoseeany replieswiththisinthemind, TCPProbing forreplyAcknowledgment Packetwhich intelligently craft/appendTCPacknowledgement messagestogiveanother layerof protection. Inthis methodextra specificationisappendedwiththe acknowledgementthatistochangetheTCPwindow sizeorcause packetretransmission.

Bernstein (2007) explains "that tomitigatetheSYNfloodingattackSYNcookiesisused" Bernstein, 2007, p.190).SYN cookieswork to alleviateSYN floodsby calculatingcookiesthatarefunctionsof the source address, source port, destination address, destination portandrandom

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

secretseed.Onreceiving SYNpacket the servercalculatesaSYNcookieandsendsit backto clientaspartof the SYN+ACKanddonotallocate resourcesfortherequestsendbyclient. When ACK packet is received theconnection is established ifa validcookieispresentin theACKpacket.SYNcachealsoused tomitigate thefloodingattacks,itusestheconceptofbacklogqueue,aminimumamount ofstate isstoredforeach SYNrequest. Bharathi et al (2010) explained that “Hop-CountFilteringusesthehopcount ofpackets arrivingat aparticularserver”. This method maps IP addresstohop counts, incase ofspoofedpackethop count of the respected packet will not match the expected hop count. HCF onlyfiltertraffic ifsome thresholdamountof packetsdoesnotmatchtheir expectedhop counts.(Bharathi et al 2010, p.120)

Ma, (2005) AwaytomitigateIP-spoofingIPpuzzlesareused, it provides active defense against IP-spoofing, in whichserversendsanIPpuzzletotheclient, nowclient needtosolvethepuzzle,ifsolutionby clientiscorrect, thenonly serverallow toconnectandstartthedata transfer.Kavisankar,&Chellapan (2011) explains that “Modernoperatingsystem comeswiththesufficient backlog queue, thesizeofbacklog queuecanbe increasedasperrequirements.Increasing thebacklog queuesimply createsmoreresourcesfortheserverto accommodatemoreTCPrequestinhalfopen state” (Kavisankar,&Chellapan, 2011, p.154).

```
 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’codeforSYNflood(Kavisankar, and Chellapan, 2011)

Hererandomfunction is used togenerate anewIP addressevery time,bywhichSYNpacketseemstobe comingfromdifferentsources.

Sendtofunctionused forsend thesyn packet to the server.

7. PacketCapturing

Dolor (2006) ThepacketsarecapturedusingWireshark,whichis a networkpacketcapturerinLinuxandwindows environment.A packetcapturer,likeWiresharkallows ustocaptureanddisplaynetworkpacketsdetails.In thispaperWiresharkisused toascertainthatour packetgenerator(theCscript)generatesSYNpackets, tocollectstatisticsontheSYNpacketsprocessedby thevictimserver,monitorTCPservicerequestsentby thedifferentclientmachines.

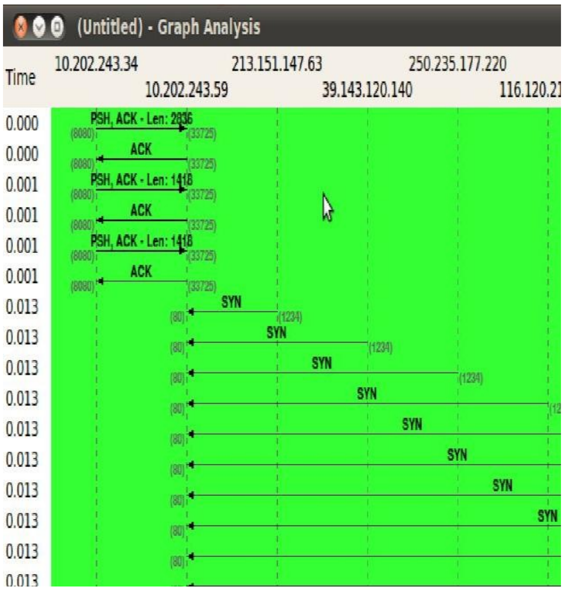

Figure 6.SYNpacketsreceivedonvictimserver. (Kavisankar, and Chellapan, 2011)

Figure6showsonly SYNpacketsarereceivedatthe server end from different IP addresseswithone secondtimeinterval.

8. DetectionofSYNFloodonHost

Kavisankar,&Chellapan (2011) explains that "SYNfloodattackcanbedetectedbymonitoringthe TCPstates,netstatisthe commandbothinLinuxand Windowsenvironmentusedtodisplay thestatusof networkconnectionsin thehost.

The half open connections in Linux is encoded as SYN_RECVstate only" (Kavisankar,Chellapan, 2011, p.158).

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

$netstat–n –p –t|grepSYN_RECV|wc –l

Abovecommandcancountthe numberofhalfopen connectionsinasystematthatinstant.

9.NumberofPackets CapturedatVictim Machinewithno Attack

Figure7showsthe number of packetsonamachine capturedbywireshark,we filterpacketsby tcp.analysis.ack_rtt,resultshows maximum5 to10 packetsarecaptured at thenetwork interface ofthe servermachine.

Figure7. Totalnumber of packets per second receivedonvictimserverwithno attack. (Kavisankar, and Chellapan, 2011P. 151)

10. NumberofPacketsCapturedat Victim MachinewithSynFlood Attack

Figure8 shows the numberof packets on a victim server captured byWireshark, wefilter packets by tcp.analysis.ack_rtt, result shows 2000 to 7000 packets arecaptured at thenetwork interface ofthe servermachine. Inthisway SYNfloodattackconsume the network bandwidthandresources onthe victim machine.

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

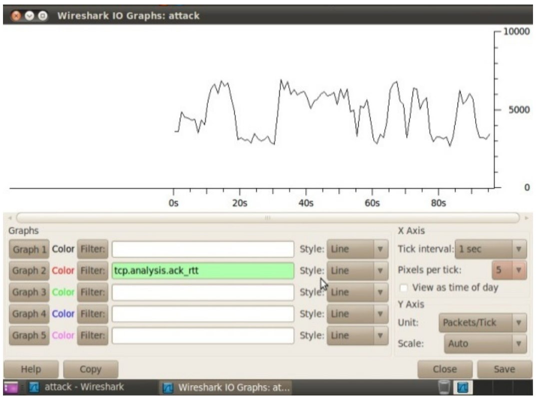

Figure 8.Total number of packets per second receivedonvictimserverwithSYNfloodattack. (Kavisankar, and Chellapan, 2011)

11. TCPSYNFloodingMitigations

a. Kavisankar ,&Chellapan,(2011) explained that **TCPProbingforReplyAcknowledgementPacket** is themethodsusedforthemitigationofTCPSYN flood with IP spoofing" (Kavisankar,Chellapan, 2011, p.152). The sender ofspoofing packets mostly unabletoseeany replywiththisinthemind, TCPProbing forreplyAcknowledgment Packetwhich intelligently craft/appendTCPacknowledgement messagestogive another layerof protection.Inthis methodextra specificationisappendedwiththe acknowledgementthatistochangetheMa (2005) TCPwindow sizeorcause packetretransmission.Inthismethodserver sendsSYN+ACK+craftmessagetoclientback,theresultfrom thelearning/recording packetanalyzer, checkswhether theTCPreply acknowledgement packet satisfies the specification givenby theserverusingTCPprobing tochangethe TCPwindowsize.

b. **IncreasetheBacklog QueueoftheServer:** Postel, (1999) InThismethodwesimplyincreasethebacklogqueue of the servertomaintainmore halfopenconnections, tcp_max_syn_backlogis the parameter to set in the mostlyLinuxoperatingsystem.

c. **SYN Cookies:** Bernstein, (1997) points out that "TomitigatetheSYNfloodingattackSYNcookiesis used".SYN cookieswork to alleviateSYN floodsby calculating cookies that are functions of the source address, source port, destination address, destination portandrandom secretseed.OnreceivingSYNpacket the servercalculatesaSYNcookieandsendsit backto clientaspartof the SYN+ACKanddonotallocate resourcesfortherequestsendbyclient. Kirkland (2000) points out that "WhenACK packet is received theconnection is established ifa validcookieispresentintheACK packet" .TheTCP parametertcp_syncookiesinLinuxisdirectlyinvolved inmitigationofSYNfloodattack.

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

12. ConclusionandFutureWork

Inthispaperwesuccessfully providedasimple experiment to producea TCPSYNfloodingDDOS attack,weestimatethepacketrateonavictimserver persecond. We look at the devastation flooding can cause to an organization and the various approaches to sync flood attacks. We also outlined some steps that can be taken by organizations to mitigate against syn attacks on web servers or other network resources.

As a way of further studies,welikeresearchers toanalyzeandprovide solutionstothe several floodingattackson network likeUDP floodingetc.,in bothwiredandwireless

References

BharathiKrishnaKumar,P.KrishnaKumar (2010) "Hop CountBased Packet ProcessingApproachto CounterDDoSAttacks" InternationalConference onRecentTrendsinInformation, TelecommunicationandComputing,

D. Kirkland, (2000) TCP protocol

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

Dolor (2006) Computer Hacking and packet capture. (Mastersthesis University of louxembourge). Retrieved fromwww.wireshark.org

J.Postel, (1999) "TransmissionControlProtocol", RFC793,9/81.

L. Kavisankar,C.Chellapan, (2011) "AMitigationmodelforTCP SYNflooding withIPSpoofing",IEEE-International Conference on Recent Trends in InformationTechnology, ICRTIT2011,pp.251-256.

Ma,M, (2005)"Mitigating denialofserviceattackswithpassword puzzles" inInformationTechnology:CodingandComputing, Vol.2,May 2005.pp.621- 626.

RFC (1996) TCPSYNfloodingand commonmitigation.

Stopforth,Riaan: (2007)Techniquesandcountermeasures of TCP/IP OSfingerprintingonLinuxSystems,Thesis, Universityof KwaZulu-Natal,Durban,