International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

An Experimental Work Of TCP SYN Flood Ddos Attack On Cloud Environment – Simulation Approach

C.Bagyalakshmi[1] [0000-0001-6630-3678], Dr.E.S.Samundeeswari[2] [0000-0002-1783-2634] and V.Arun kumar[3] [0000-0002-1399-9437]

[1 & 2] Vellalar College for Women, Erode, Tamilnadu.
[3]Kongu Engineering College, Erode, Tamilnadu.

[1]bagyachithra@gmail.com

Abstract. Cloud data is facing enormous security issues now a days. Security issues are like data attack or hijack of data in cloud environment. Major attack scenario is about DDoS attack, it suppresses the data service permanently or some more time to deny the service. The real time practical approach could not be carried out because cost of network and its hardware infrastructure erection is very high. Hence, to overcome DDoS attack problem, a simulation approach is carried out in this paper. This work is simulated using virtual box with Kali Linux and Windows OS, to generate SYN packets from Kali Linux OS (attacking machine) and receive the packets to Windows OS (victim machine).

Keywords: Cloud Computing, DDoS attack, SYN flood

1. INTRODUCTION

The Internet become more popular because increasing in usage of digital platforms by enterprises, schools and healthcare. The Client or Server activities like storing, retrieving and transferring data to anywhere increase the Internet usage day by day. Network speed, bandwidth and prices are nominal for people at present, at the same time network issues are raising either with storage issues or communication problem etc., Hence to overcome the issues in a friendly and flexible way to the user's, new technology called cloud computing is introduced [1]. Cloud computing helps to retrieve, store and transfer the data in easy way.

Cloud computing is a pay-per use model, it has classified into four types, there are Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud. Each cloud types have their own circumstances and data limit also. Cloud services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud service provider plays an important part in cloud technology[2]. Cloud provider decides the storage level and access to users, provider also concentrates about privacy and security.

Security issue is one of the disadvantage of cloud. The most common security issue is Denial of Service (DoS) attack, it could be denied the service and causes severe damage to the entire system. In such a way another one is Distributed Denial of Service (DDoS) attack, it consumes more bandwidth and denies the legitimate user services [5].

DDoS attack concentrate towards the demolishing of entire system or network activity and creates more traffic in network which causes loss of data. DoS attack is classified into three types, Volume based, Protocol based and Application based. Volume based attacks could be attacked through servers with ICMP flood and UDP flood which are involved in this category. The specific protocol to consume the servers resources are followed in Protocol based attack. TCP-SYN flood and Ping of Death (PoD) attacks are Protocol based attack [3]. Application layer attack targets the system applications, Slow Loris attack and DNS amplification attack are examples of application based attack.

1.1 TCP-SYN Flood Attack

The Transmission Control Protocol/Internet Protocol (TCP/IP) model has 7 layers, Source and destination connection through TCP/IP layers[7]. The connection is established from layer one to layer seven, the data is transferred from each layers. To exchange the data from source to destination through TCP connection, is a standard method to establish a network conversation.

The data packets are send by IP with the help of TCP [4]. The state of TCP connection is indicated by flags, it gives some additional or useful information like troubleshooting or handling the connections. TCP flags consists of Synchronization (SYN**),** Acknowledgement (ACK**),** Finish **(**FIN**),** Reset (RST**),** Push (PSH**)** and Urgent (URG**).** Commonly used flags are SYN, ACK and FIN and each flag carries one bit for each transaction. The data packets are exchanged between sender and receiver for TCP three way handshake process. Three way handshake process as shown in (Figure 1) are SYN, SYN- ACK and ACK.

A ------------------SYN----------------- > B
A <---------------SYN/ACK--------------B
A ------------------ACK ----------------> B

Figure 1: TCP Handshake Process

Two hosts A and B, are used to exchange the information through TCP connection. First, A sends the SYN packets to B. B receives SYN packets and sends it back to SYN- ACK packets and then to A [6][9]. Finally A receives the ACK packets from B, now the connection is established through proper channel. The above mentioned process is continued with their order, perhaps this process could be disturbed by illegal users and lead to loss of connection in both sender and receiver.

The client and server connections are established through TCP handshake, it set flags are SYN and ACK to exchange the message for communication in normal way (Figure.2 (a)). A very common DDoS attack is SYN attack, which simply sends a large number of SYN packets and never acknowledge any of the replies and blasting the service with such a large number of meaningless requests (Figure.2 (b)) that grave users are unfit to use it.

TCP-SYN flood attack is protocol based DDoS attack, it sends more number of SYN packets to the target system or server [8]. SYN flood attack deny the particular service or system and consumes more bandwidth so it is also called as Bandwidth attack. When server receives more SYN packets at that time legitimate users could not access the particular server, it is little harmful attack.

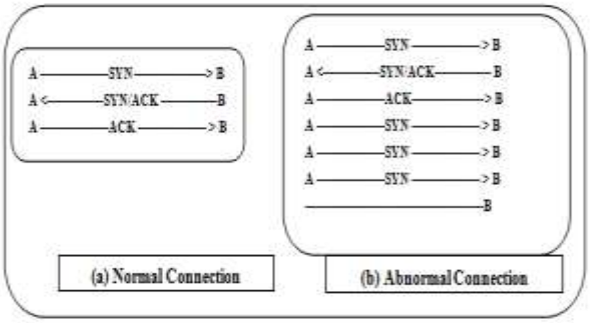


Figure 2: TCP-SYN Flood Attack

The objective of the work, to overcome the TCP-SYN flood attack in cloud environment and to detect these type of attack patterns or behaviors. To develop Intrusion detection model for TCP-SYN flood attack in cloud environment, so that it can focus on simulation approach.

2. BACKGROUND STUDY

Shilpi Gupta et.al.,(2012) Secure data transmission is carried out using appropriate intrusion detection method. Wireshark tool is used for intrusion detection system, two methods of intrusion detection system is followed they are host based and network based. The experimentation connections are established through TCP and UDP. To identify different types of intrusions in various networks used Wireshark.

Zouheir Trabelsi et.al., (2013) As a part of ethical hacking experimentation is carried out in lab scale[9]. This experiments explains about the development of defensive technique against DDoS attack is generated by snort tool, it is open source tool. In snort tool, attack signatures are disclosed which helps in detecting attack packets. Ethical hacking through snort rule is based on rule header and rule options. The LAN experimentation is made with two Windows based OS and generate snort rules for attack.

Dambar pun et.al., (2015) Tried to experiment SYN flood attack in wired topology network**.** Major network security issues like SYN packet flood attacks are created and tested with DNS server attack[10]. Due to increase in network traffic users are facing difficulties with handling of malicious data. Continuous monitoring of traffic is necessary for the troubleshooting of network issues[11]. Large number of data packets are send through SYN packets while sending this data acknowledge signal will not be received during this attack.

Bo Chen et.al.,(2015) Data security system for real time cyber physical system is developed and implemented in this work. Vulnerabilities of real time system and supervisory control data acquisition system is used. Simulation of this cyber physical system is developed by using open net system in loop concept. Component architecture along with their data flow are discussed which includes mitigation of vulnerabilities in real time system are discussed.

Khalid Hussain et.al .,(2016) Honeypot is a method of increasing the data security by introducing some open ports to hackers which attracts the malicious data set and diverts the real data from hacking. A new type of three way counter algorithm is proposed in this work to improve the firewall capability in identifying the SYN flood attack is proposed. Software tools like Ettercap, hping3 and Wireshark are used. To generate SYN flood attack in the network using LAN Ettercap tool, analysis is carried out using Wireshark. SYN flood attack is mitigated in this work similar to DDOs attack.

Nick Gregoriol et.al.,(2019) Cloud technology has grown well nowadays which makes the utilization of virtual machines from single machine, at the same time risk towards the usage of data is increasing, Experimentation on legal SYN flood attack using spoofed internet resource in legal SYN flood attack. In this work kali Linux, AWS and google cloud platform are used.

Simulation of TCP SYN Flood Attack

Cloud environment facility is provided by third parties, they needs to provide security for user’s data. Now a days many cloud providers are available in the market, but users are unable to find the authenticity of service providers, at the same time intruders also increasing day by day. Hence to trace the network activity or patterns and behaviors to avoid network traffic and to find the solution for this network traffic issue. This work explains about protocol based DDoS attack and to generate the attack through simulation approach.

Here, virtual cloud environment is created by Virtual box and installed with two virtual operating systems like Kali Linux and Windows. Kali Linux is attacking machine and windows is a victim machine. The DDoS attack process is experimented between these two operating systems[12]. Wireshark tool is installed in victim machine (windows).The SYN packets are generated from attacking machine (Kali) using hping3 command. Hping3 is a tool, to generate more number of SYN packets within a specified time duration [13]. When victim machine receives SYN packets, at that time connection could not be established with particular server or system, mean while Wireshark tool captures the network activities. Wireshark log file is helps to find the network activities and behavior [11].

Virtual box is developed by Oracle Corporation and open source tool and user friendly, to manage operating systems like Windows, Linux, mac and Solaris. All kind of ISO files are available in internet[13]. Figure 3 shows two virtual machines are installed in virtual box.

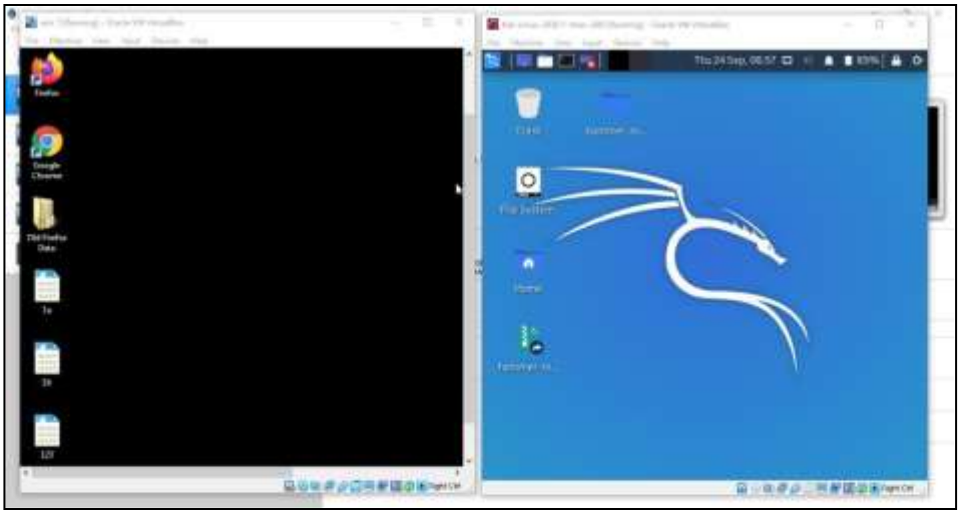
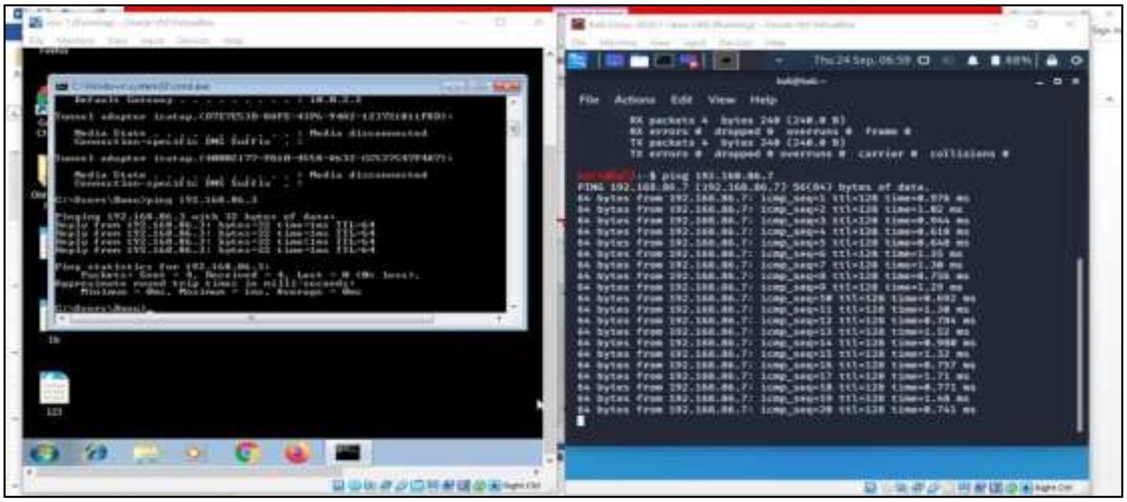


Figure 3: Virtual Machines using Virtual Box Tool

Windows OS and Kali Linux OS is installed in virtual box tool. Windows machine is acted as victim machine and Kali machine is acted as attacking machine.



```
   Default Gateway . . . . . . . . . : 10.0.2.2

Tunnel adapter isatap.{[illegible]}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{[illegible]}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\[illegible]>ping 192.168.86.3

Pinging 192.168.86.3 with 32 bytes of data:
Reply from 192.168.86.3: bytes=32 time<1ms TTL=64
Reply from 192.168.86.3: bytes=32 time<1ms TTL=64
Reply from 192.168.86.3: bytes=32 time<1ms TTL=64
Reply from 192.168.86.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.86.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\[illegible]>
```

```
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[illegible] $ ping 192.168.86.7
PING 192.168.86.7 (192.168.86.7) 56(84) bytes of data.
64 bytes from 192.168.86.7: icmp_seq=1 ttl=128 time=0.976 ms
64 bytes from 192.168.86.7: icmp_seq=2 ttl=128 time=1.02 ms
64 bytes from 192.168.86.7: icmp_seq=3 ttl=128 time=0.944 ms
64 bytes from 192.168.86.7: icmp_seq=4 ttl=128 time=0.610 ms
64 bytes from 192.168.86.7: icmp_seq=5 ttl=128 time=0.640 ms
64 bytes from 192.168.86.7: icmp_seq=6 ttl=128 time=1.35 ms
64 bytes from 192.168.86.7: icmp_seq=7 ttl=128 time=1.30 ms
64 bytes from 192.168.86.7: icmp_seq=8 ttl=128 time=0.756 ms
64 bytes from 192.168.86.7: icmp_seq=9 ttl=128 time=1.29 ms
64 bytes from 192.168.86.7: icmp_seq=10 ttl=128 time=0.692 ms
64 bytes from 192.168.86.7: icmp_seq=11 ttl=128 time=1.30 ms
64 bytes from 192.168.86.7: icmp_seq=12 ttl=128 time=0.784 ms
64 bytes from 192.168.86.7: icmp_seq=13 ttl=128 time=1.52 ms
64 bytes from 192.168.86.7: icmp_seq=14 ttl=128 time=0.980 ms
64 bytes from 192.168.86.7: icmp_seq=15 ttl=128 time=1.32 ms
64 bytes from 192.168.86.7: icmp_seq=16 ttl=128 time=0.757 ms
64 bytes from 192.168.86.7: icmp_seq=17 ttl=128 time=1.71 ms
64 bytes from 192.168.86.7: icmp_seq=18 ttl=128 time=0.773 ms
64 bytes from 192.168.86.7: icmp_seq=19 ttl=128 time=1.40 ms
64 bytes from 192.168.86.7: icmp_seq=20 ttl=128 time=0.741 ms
```

Figure 4: Normal Connection checking using Ping Command

Ping command is tested for network connection (figure 4) from both the machines. Both machines are connected through virtual adapter, provided by virtual box.

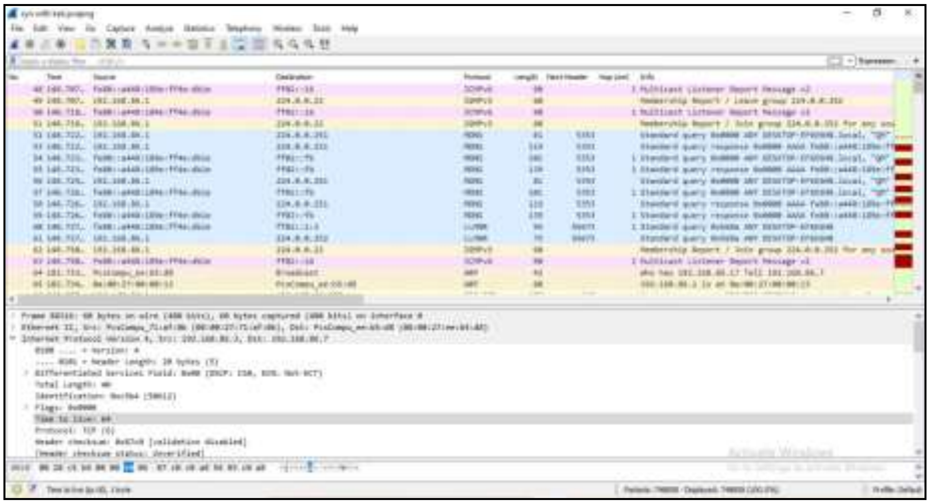
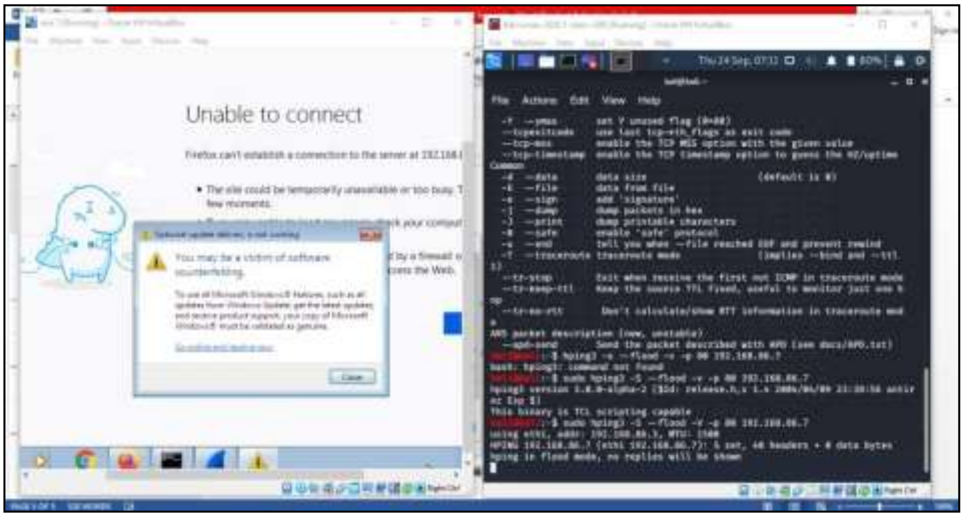


Figure 5: Normal Network Process Captured by Wireshark

Wireshark is open source tool and user friendly to analyse the statistics information about network and packets[14]. Additionally, it helps to find and improve the packets flow, packets information, protocol information etc., Figure 5 shows that normal network activity of virtual machines.



Unable to connect

Firefox can't establish a connection to the server at 192.168.[illegible]

- The site could be temporarily unavailable or too busy. T[illegible] few moments.
- [illegible] check your comput[illegible]
- [illegible] by a firewall o[illegible] cess the Web.

You may be a victim of software counterfeiting.

To use all Microsoft® Windows® features, such as all updates from Windows Update, get the latest updates and receive product support, your copy of Microsoft Windows® must be validated as genuine.

```
  -Y  --ymas         set Y unused flag (0x80)
  --tcpexitcode      use last tcp->th_flags as exit code
  --tcp-mss          enable the TCP MSS option with the given value
  --tcp-timestamp    enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data         data size                      (default is 0)
  -E  --file         data from file
  -e  --sign         add 'signature'
  -j  --dump         dump packets in hex
  -J  --print        dump printable characters
  -B  --safe         enable 'safe' protocol
  -u  --end          tell you when --file reached EOF and prevent rewind
  -T  --traceroute   traceroute mode                (implies --bind and --ttl
1)
  --tr-stop          Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl      Keep the source TTL fixed, useful to monitor just one h
op
  --tr-no-rtt         Don't calculate/show RTT information in traceroute mod
e
ARS packet description (new, unstable)
  --apd-send         Send the packet described with APD (see docs/APD.txt)
[illegible]:~$ hping3 -s --flood -v -p 80 192.168.86.7
bash: hping3: command not found
[illegible]:~$ sudo hping3 -S --flood -v -p 80 192.168.86.7
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antir
ez Exp $)
This binary is TCL scripting capable
[illegible]:~$ sudo hping3 -S --flood -V -p 80 192.168.86.7
using eth1, addr: 192.168.86.3, MTU: 1500
HPING 192.168.86.7 (eth1 192.168.86.7): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 6: To Generate SYN flood Attack using hping3 Command

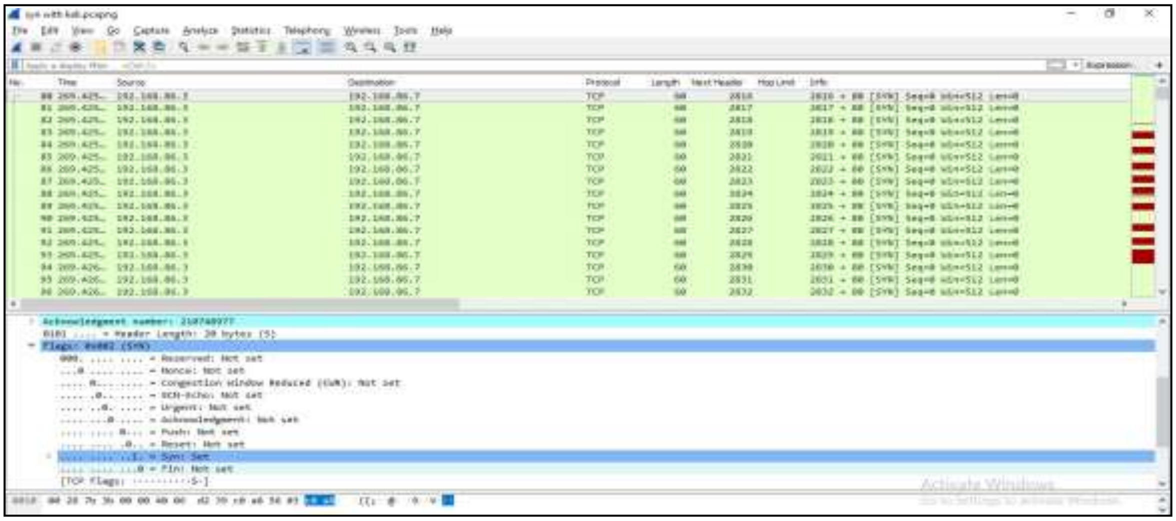
Attacking machine is ready to generate the SYN packets to the target machine (Figure 6). The SYN packets are generated using hpin3 tool. Hping3 tool is inbuilt in Kali OS, hence it can generate packets easily[15]. Hping3 command for generating the packet is,

Hping3 –S –flood –V –p port number victim machine IP address

above command to generates SYN packets successfully and it reaches to victim machine. Victim machine could not access their network activity until hping3 command is stopped.

The SYN packets are generated and captured by Wireshark tool (Figure 7), to analyse network behaviors. SYN attack is one of the DDoS attack, it is protocol based attack, consumes more bandwidth size and deny the service some more time.

Flow graph expresses about the SYN flags connectivity between both machines (Figure 8). This graph visualizes clearly and explains about TCP hand shake process and it could identify the movement from source to destination easily.



syn with kali.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Activate Windows

```
No.  Time        Source         Destination    Protocol Length Next Header Hop Limit Info
  80 269.425…   192.168.86.3   192.168.86.7   TCP      60     2816                  2816 → 80 [SYN] Seq=0 Win=512 Len=0
  81 269.425…   192.168.86.3   192.168.86.7   TCP      60     2817                  2817 → 80 [SYN] Seq=0 Win=512 Len=0
  82 269.425…   192.168.86.3   192.168.86.7   TCP      60     2818                  2818 → 80 [SYN] Seq=0 Win=512 Len=0
  83 269.425…   192.168.86.3   192.168.86.7   TCP      60     2819                  2819 → 80 [SYN] Seq=0 Win=512 Len=0
  84 269.425…   192.168.86.3   192.168.86.7   TCP      60     2820                  2820 → 80 [SYN] Seq=0 Win=512 Len=0
  85 269.425…   192.168.86.3   192.168.86.7   TCP      60     2821                  2821 → 80 [SYN] Seq=0 Win=512 Len=0
  86 269.425…   192.168.86.3   192.168.86.7   TCP      60     2822                  2822 → 80 [SYN] Seq=0 Win=512 Len=0
  87 269.425…   192.168.86.3   192.168.86.7   TCP      60     2823                  2823 → 80 [SYN] Seq=0 Win=512 Len=0
  88 269.425…   192.168.86.3   192.168.86.7   TCP      60     2824                  2824 → 80 [SYN] Seq=0 Win=512 Len=0
  89 269.425…   192.168.86.3   192.168.86.7   TCP      60     2825                  2825 → 80 [SYN] Seq=0 Win=512 Len=0
  90 269.425…   192.168.86.3   192.168.86.7   TCP      60     2826                  2826 → 80 [SYN] Seq=0 Win=512 Len=0
  91 269.425…   192.168.86.3   192.168.86.7   TCP      60     2827                  2827 → 80 [SYN] Seq=0 Win=512 Len=0
  92 269.425…   192.168.86.3   192.168.86.7   TCP      60     2828                  2828 → 80 [SYN] Seq=0 Win=512 Len=0
  93 269.425…   192.168.86.3   192.168.86.7   TCP      60     2829                  2829 → 80 [SYN] Seq=0 Win=512 Len=0
  94 269.426…   192.168.86.3   192.168.86.7   TCP      60     2830                  2830 → 80 [SYN] Seq=0 Win=512 Len=0
  95 269.426…   192.168.86.3   192.168.86.7   TCP      60     2831                  2831 → 80 [SYN] Seq=0 Win=512 Len=0
  96 269.426…   192.168.86.3   192.168.86.7   TCP      60     2832                  2832 → 80 [SYN] Seq=0 Win=512 Len=0

  > Acknowledgment number: 210740977
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]

0010  00 28 7e 3b 00 00 40 06  d2 39 c0 a8 56 03 c0 a8
```

Figure 7: TCP-SYN Flood Attack Captured by Wireshark

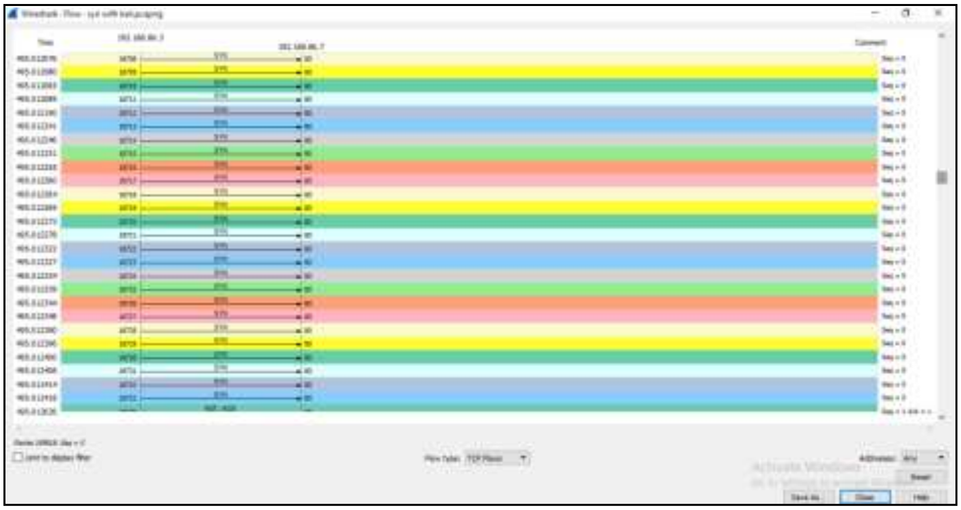


Figure 8: Flow graph of TCP-SYN Attack using Wireshark

3. CONCLUSION

DDoS attack using simulation approach is discussed in this work. TCP-SYN flood attack is a three way handshake process of TCP connection. TCP protocol flag is set as SYN, it could not make connection to target system or network. It denies the service some
more time to users. Hence legitimate users could not make connection. This experimental study is carried out using virtual box, with two virtual machines were created, one is attacking machine (Kali) and another one is victim machine (Windows). SYN packets were generated from attacking machine to target machine through hping3 tool. Packets are captured by Wireshark tool. This study helps to find a practice on more number of experimentation towards cyber attacks. This experimentation will generate awareness and supports detailed study towards cloud

data security in future.

4. FUTURE WORK

Artificial Intelligence is growing technique. AI techniques are used in many fields like health care, industries, education etc., Cyber security is key issue in cloud environment. This type of experimentation could follow the behavior and pattern of network activity which helps to identify the intruders easily. Hence, to develop Intrusion Detection System (IDS) based on AI techniques also to detect different type of attacks in cloud environment, is a key way of identifying either normal or abnormal activities. It will minimize the burden of risk towards cloud data security.

5. REFERENCES

[1]. Bo Chen., Nishant Pattanaik ., Ana Goulart., Karen L. Butler-Purry., & Deepa Kundur, “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed” In *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR),* 1-6, (2015).

[2]. Dambar pun., Batajoo amit., & Bishnu Prasad gautam,“Vulnerability of Network Traffic in Data Centers under Various kinds of Attacks” In *IPSJ SIG Technical Report*, 62(16), 1-5, (2015).

[3]. Deepak Singh Rana., Naveen Garg., & Sushil Kumar Chamoli, “A Study and Detection of TCP

[4]. SYN Flood Attacks with IP spoofing and its Mitigations” In *International Journal of Computer Technology and Applications*, *3*(4), 1476-1480, (2012).

[5]. Florian Bartholomae, “Cybercrime and cloud computing. A game theoretic network model” In

[6]. *Managerial and Decision Economics*, *39*(3), 297-305, (2018).

[7]. Khalid Hussain, Syed Jawad Hussain, Veena Dillshad, Muhammad Nafees & Muhammad Awais Azeem, “An Adaptive SYN Flooding attack Mitigation in DDOS Environment” In *International Journal of Computer Science and Network Security (IJCSNS)*, *16*(7), 27-33,(2016).

[8]. Mohammed Abdul Qadeer , Mohammad Zahid , Arshad Iqbal Scientist B & MisbahurRahman Siddiqui , “Network traffic analysis and intrusion detection using packet sniffer” In *2010 Second International Conference on Communication Software and Networks - IEEE,* 313-317, (2010).

[9]. Nick Gregorio, Janahan Mathanamohan, Qusay H. Mahmoud, May altaei, “Hacking in the cloud” In *Internet Technology Letters*, *2*(1), 1-6,(2019).

[10]. Shilpi Gupta & Roopal Mamtora, “Intrusion detection system using wireshark” In *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(11), 358-363, (2012).

[11]. Sushil K. Sharma & Joshua Sefchek, “Teaching information systems security courses: A hands- on approach” In *Computers & Security*, *26*(4), 290-299. (2007).

[12]. Dr. Zouheir Trabelsi & Latifa Alketbi,” Using network packet generators and snort rules for teaching denial of service attacks” In *Proceedings of the 18th ACM conference on*

Innovation and technology in computer science education, 285-290,(2013).

[13]. Wireshark packet analyzer Available: https://www.wireshark.org/

[14]. TCP SYN Flooding and IP Spoofing Attacks. Available: http://www.cert.org/historical/advisories/ca-1996-21.cfm?

[15]. Hping3 packet generator and analyzer. Available: http://linux.die.net/man/8/hping3.

[16]. Sujatha, K & Shalini Punithavathani, D 2016, ‘Fuzzy Based Weight Estimation and Sub band Architecture in Image Fusion for Multi Exposure Images’, Asian Journal of Information Technology (AJIT), ISSN:1682-3915, Vol. 15, No.3, pp.384-392.

[17]. Viji, C., Rajkumar, N., Suganthi, S.T. et al. An improved approach for automatic spine canal segmentation using probabilistic boosting tree (PBT) with fuzzy support vector machine. J Ambient Intell Human Comput (2020).