RESEARCH ARTICLE OPEN ACCESS

Detection of ICMP Flood DDoS Attack

Harshita [1], Ruchikaa Nayyar [2]
Department of Information Technology
IGDTUW
New Delhi - India

ABSTRACT

The term denial of Service (DOS) refers to form an attacking computers over a network. The denial of service attack is an explicit attempt by an attacker to prevent the legitimate users not to access the services. When this attack is made at a larger amount that is by using multiple computers than it's known as Distributed Denial of Service Attack (DDoS) [1]. An attacker can use many techniques for denial of service like flooding technique is to flood a network and reduce the legitimate user bandwidths to disrupt the services of the users. In DDoS attack, the attacker try to interrupt the services of a server and utilizes its CPU and Network. Flooding DDOS attack is based on a huge volume of attack traffic which is termed as a Flooding based DDOS attack. Flooding-based DDOS attack attempts to congest the victim's network bandwidth with real-looking but unwanted IP data. Due to which Legitimate IP packets cannot reach the victim because of lack of bandwidth resource [5]. ICMP FLOOD initiated by sending a large number of ICMP packets to a remote host. As a result, the victimized system's resources will be consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients. In this research firstly, we detect the ICMP Flood by using various methods and tools and find out what are the different parameters on which ICMP flood DDoS attack happens.

***Keyword*:-** Denial of Service (DoS), Distributed Denial of Service (DDoS), ICMP, Echo Request.

I. INTRODUCTION

Denial of Service Attack (DoS) and Distributed Denial of Service Attack (DDoS) have become a major threat to present computer networks. DDoS is a kind of attack in which attacker target the victim network resources such as bandwidth, memory etc. so that victim may stop responding legitimate users [2]. DoS and DDoS attacks attempts to make a machine unavailable for the authorized users. In DoS or DDoS attacks attacker used to send bogus requests to intended users to make the services unavailable to the authorized users or just crashes the system means attacker used to overload or flood the target machine. DDoS attacks are a global threat and not limited to any specific industry verticals. The largest DDoS attack of 2015 was measured more than 240 gigabits per second and persisted for 13 hours. [15]

A. *The main purpose to perform DDoS attack is to effect the following are*

1) Consumption of computational resources, such as bandwidth, disk space, or processor time.
2) Disruption of configuration information, such as routing information.
3) Disruption of state information, such as unsolicited resetting of TCP sessions.
4) Disruption of physical network components.

B. *DDoS attacks are divided mainly into three types*

1) Volume based attacks: Volume based attacks includes UDP, ICMP flood attack. In this attack, attacker's aim is to Saturates the bandwidth of the victim's side. Here bandwidth means the no of data or packets send per second. So the bandwidth of attacker must be higher than bandwidth of the victim. Bandwidth is measured in bits per second. [6]

2) Protocol based attack: Protocol attack includes SYN Flood, Ping of Death attack, Smurf Attack. In this type of attacks attacker used to consumes the actual resources of server and this is measured in packet per second. [6]

3) Application Layer attacks: The goal of Application layer attack is to crash the web servers means consumes the application resources or services making it unavailable to others or legitimate users. These attacks are very hard to detect and mitigate. Magnitude is measured in request per second. [6]

In a DDoS Attack many applications pounds the target browser or network with fake requests that makes the system, browser, network or the site slow, useless and disabled or unavailable. DDoS attack mainly focuses on the exhaustion of network, services resources and applications thereby restricting the legitimate users from accessing their system or network resources.

C. *Techniques of DDoS attack*

There are many techniques are used to overload a system these are given below.

1) *Bandwidth Consumption:* In bandwidth consumption many techniques are used i.e. Many/large packets, ICMP flood, UDP Flood, Forge source address
2) *SYN Flooding Attacks*

3) *Application Level Flood Attack.*
4) *Permanent Denial of Service Attack*

D. Internet Control Message Protocol Flood

ICMP is a flooding attack. In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down the victim's network infrastructure. This is illustrated in Figure.

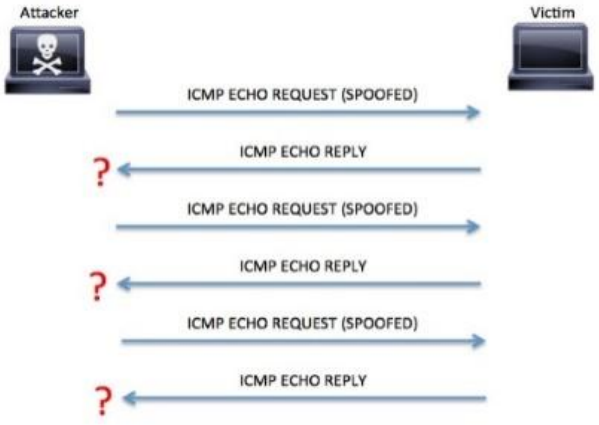
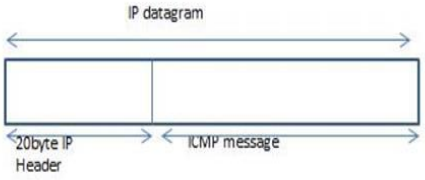


Fig.1 ICMP Flood attack

ICMP stands for Internet Control Message Protocol. It's mostly used in networking technology. ICMP is a connectionless protocol. ICMP mainly used for diagnostic purposes, error reporting or querying any server but now attackers are using ICMP protocol for sending payloads. The ICMP Flood –the sending of an abnormally large number of ICMP packets of any type can overwhelm the target server that attempts to process every incoming ICMP request.

An Internet Control Message Protocol (ICMP) flooding attack (Schuba*et al*., 1997) comprises of a stream of ICMP ECHO packets generated by the attackers and aimed at the victim. The victim replies to each ICMP request, consuming its CPU and network resources. The Smurf Attack (Alomari*et al*., 2012) is a reflector attack. The attacker directs a stream of ICMP ECHO requests to broadcast addresses in intermediary networks, spoofing the victim's IP address in their source address fields. A multitude of machines then reply to the victim, overwhelming its network.

E. ICMP packet format



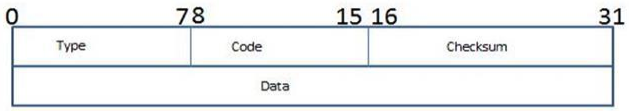


Fig.2 ICMP packet format

In the given below ICMP format the first two columns determine whether an ICMP query message or an error message. ICMP error messages are not sent in response to an ICMP error. When an ICMP error is sent, it always sends the IP header and the datagram that caused the error. So the receiving unit gets to associate the error with the process. So when a type 0 (echo reply) is sent, the reply will no longer be a Type 8 (echo request).

The last field of the ICMP format talks about the checksum. This field is used for error checking. Before an ICMP message is transmitted, the checksum is computed and is inserted into the field. So at the receiving end the checksum is calculated again and verified against the checksum field. If any mismatch is found, then it confirms that an error or change has occurred.

F. PING command

PING stands for Packet Internet Groper. It is the command which is used for testing the connection between two network nodes by sending packets and nothing in response. Nodes can be in any connection LAN, MAN, WAN. We can ping both with IP address and domain name. Format of Ping command is:

<Ping domain name/IP address>

Ping operates by sending Internet Control Message Protocol echo request packet to the server and waits for the reply. TTL value stands for time to live. The standard TTL value can reduce up to 30. If the number of routers between host and destination increases by 30 then its time out.

G. How ICMP flood DDoS attack happens:

ICMP Flood attacks exploit the Internet Control Message Protocol (ICMP), which enables users to send an echo packet to a remote host to check whether it's alive. More specifically during a DDoS ICMP flood attack the agents send large volumes of ICMP_ECHO_REQUEST packets (''ping'') to the victim. These packets request reply from the victim and this has as a result the saturation of the bandwidth of the victim's network connection. During an ICMP flood attack the source IP address may be spoofed. Attacker use IP spoofing in order to hide their true identity, and this makes the trace back of DDoS attacks even more difficult.

1) ***Practical demonstration of ICMP flood****:* Here we took 3 machine where 2 are virtual machine and 1 physical machine. Windows 8 as current machine. Kali Linux as Attacker machine. Windows 7 as target machine. To carry put ICMP flood we need to write a command hping3 - -flood –V –i eth0 <IP address of target machine> DDoS Implementation: Check the network utilization of system before

DDoS Attack. Perform DDoS attack by using h-ping command. After performing DDoS attack again check Network utilization of the system in task manager.

2) *Screenshots of DDoS:*

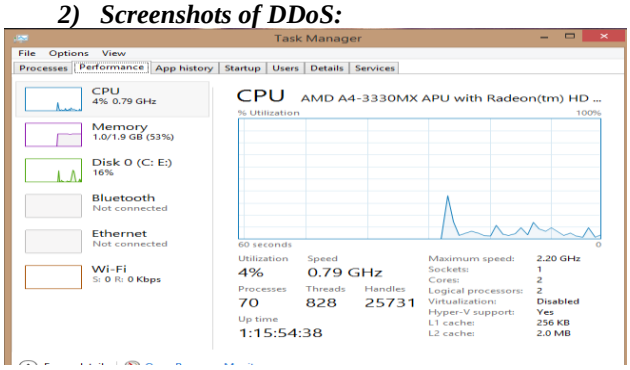


Fig 3.CPU utilization before DDoS

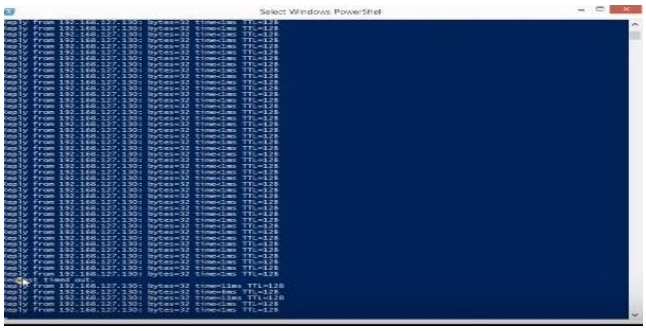


Fig.4 Performing DDoS using hping3 command

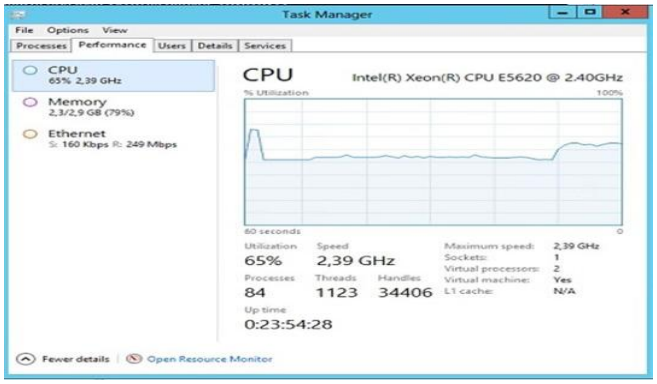


Fig. 5 Network utilization after DDoS

II. RELATED WORK

As research is going on how to avoid DDoS attacks but there are currently no successful defence against DDoS attack. But there are numerous safety measures that can be taken by the host to prevent DDoS flooding attacks. Attack prevention methods try to stop all Well Known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes. Attack prevention schemes are not enough to stop DDoS attacks because there are always vulnerable to novel and mixed attack types for which signatures and patches are not exist in the database. According to Sandeep, Ranjeet, in "study measure of DOS & DDOS"- Smurf Attack and Preventive measures configure individual host and routers not to respond to ping requests or broadcasts [1]. In the article, titled "DDA- An approach to handle DDOS attack", authors conducted the survey about DDoS attack. They discussed the various kind of DDoS such as protocol based, volume based, Application layer based [2]. A survey of defence Mechanisms against Distributed Denial of Service Flooding attack, uses hop count filtering mechanisms. In this mechanism, information about a source IP address and its corresponding hops from the destination are recorded in a table at destination site when the destination is not under attack. Once the attack alarm is raised, the victim inspects the incoming packet's source IP address and their corresponding hops to differentiate the spoofed IP packets [4]. History-based IP filtering (HIP) is another filtering mechanism that has been proposed by Peng et al in order to prevent DDoS attacks. If we use History-based IP filtering, and if the attacker knows that the IP packet filter is based on previous connections, they could mislead the server to be included in the IP address database. Victim can filter Bandwidth attack traffic according to the history they had made. However any large Scale DDOS attack that can simulates normal traffic behaviour will defeat such Mechanism [5]. According to M.A. Vinoth kumar and R. Udaya kumar, Identifying and Blocking high And low rate DDOS ICMP Flooding, they formed an algorithm in which if High rate DDOS algorithm if (I Rate > A Band) Block IP and Port Alert DDOS attack to all IPS. But the limitation is we cannot block ICMP port no because ICMP Port no is 0. ICMP do not use any port number [12]. ICMP trace back has been proposed by Bellovin, according to this mechanism every Router samples the forwarding packets with a low probability (1 out of 20,000) and Sends an ICMP trace back message to the destination. If enough trace back messages are gathered at the victim, the source of traffic can be found by constructing a chain of Trace back messages. A major issue of this approach is the validation of the trace back Packets. Although the PKI requirement prevents attackers from generating false ICMP Trace back messages, it is unlikely that every router will implement a certificate-based Scheme. We can setup our server to ignore the pings so that our server won't consume Bandwidth replying the thousands of pings that the server is receiving [8]. According to "DDoS Attack Algorithm using ICMP flood"—researcher proposed an algorithm in which they use different perimeters. It has been tested in virtually simulated environment using 5 virtual machines connected to local ISP broadband network connection. This algorithm assumes that attacker and the victim present on the same network. To perform the DoS attack they use different parameters. 1. No. of packets. 2. Packet size. 3. No of machines required for attack. 4. IP address of target machine.

But researchers already define the number of machines they use i.e.5, but we can't predefined number of machines, it depends on bandwidth of data. [13]
However, this research work is based on detecting the ICMP echo request that can cause flooding attack and based on analysis have to limit the bandwidth of the ICMP packet if bandwidth of an attacker is lesser than the target than no attack takes place. So we have to limit the bandwidth of the ICMP packet. So we can limit the threshold value up to 1000 bits/sec, if any ICMP packet exceeds this value than router will discard this value with its own.

III. METHODOLOGY

It is a process to proceed towards my research. The target is to categorise the entire research and bifurcate it into small modules. It has been divided into different modules.

A. Collection of Data

Survey on 50 different websites
10 government websites, 10 private company Websites,10Educationwebsites,10 banking websites, 10 gaming websites
Start pinging all these website using ping command

B. Gathering Information

After pinging, collect as much as information you can.
IP address
TTL
Response time
Use ping -l packet size -t IP address command to change default packet size
Use trace route command for tracing the route of the site.

C. Conclusion

By collecting data and gathering information, I gathered many perimeters and by using that parameters I will propose an algorithm for DDoS attack using ICMP flood.

In this research work we have done the survey of 50 different sites i.e. 10 government sites, 10 banking sites, 10 education sites, 10 gaming sites, 10 private company sites, Pinged the sites by using ping command i.e. ping<target IP address/company name>.

IV. SURVEY

As previously mentioned in methodology survey of 50 sites has been done. In survey part we are showing the survey of different sites and according to this survey different conclusion has been made. Through this conclusion the final result has been concluded.

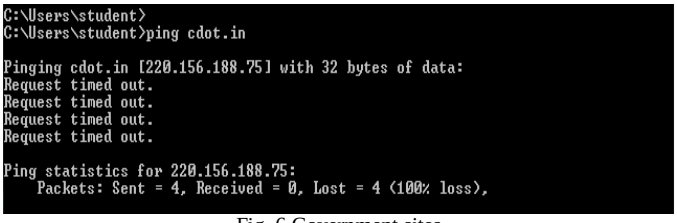


Fig. 6 Government sites

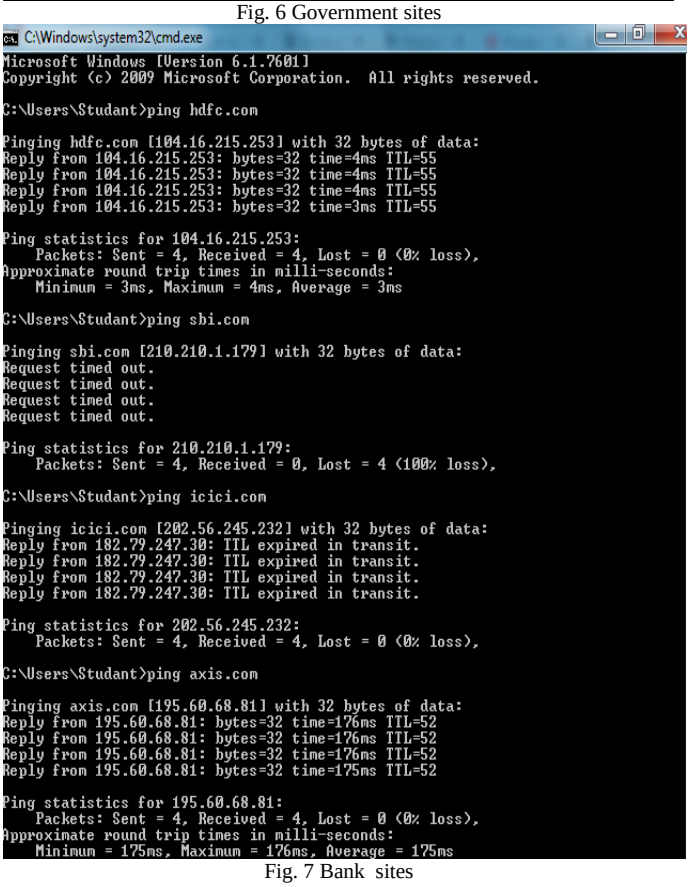


Fig. 7 Bank sites

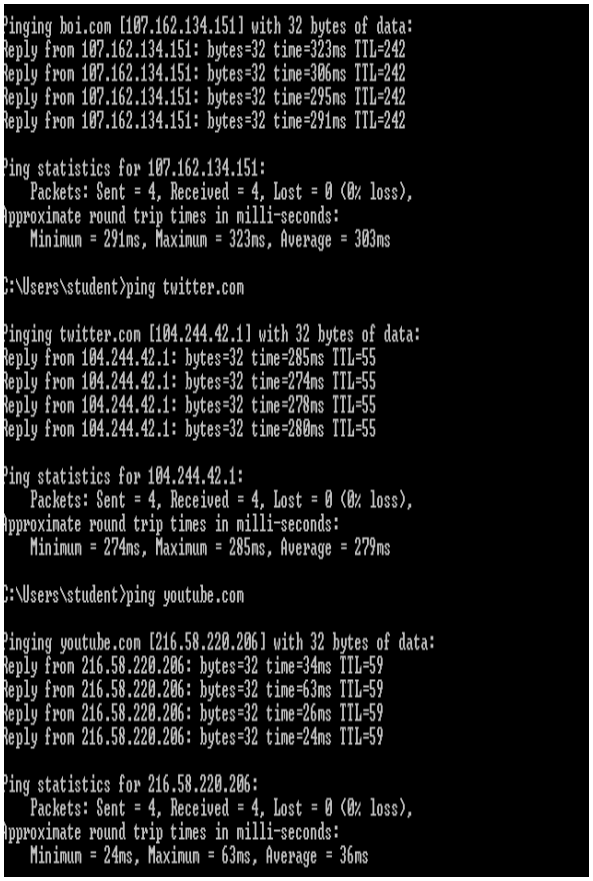


Fig. 8 Private company sites

After Pinging different site, got different parameters.

IP address
Time
TTL (Time to live)
Minimum, Maximum and Average time.

Some site has disabled the ICMP packet and their reply is RTO (Request Time Out).

Time: Time parameter tells us in how much time response came back. If response time is >100ms it means there are more than 10 hops between source and destination.

TTL: TTL parameter tells us about the Operating System used worldwide
If TTL=32, Old nux operating system
If TTL=64, Nux family
If TTL=128, Windows operating system
If TTL= 255, Old windows based routers.

In windows the default ICMP packet size is 32 bytes, but the packet size range is from 0-65500 in windows. ICMP flood DDoS Attack can be performed by increasing the default packet size
By using**: ping –l packet size –t IP address of target machine.**

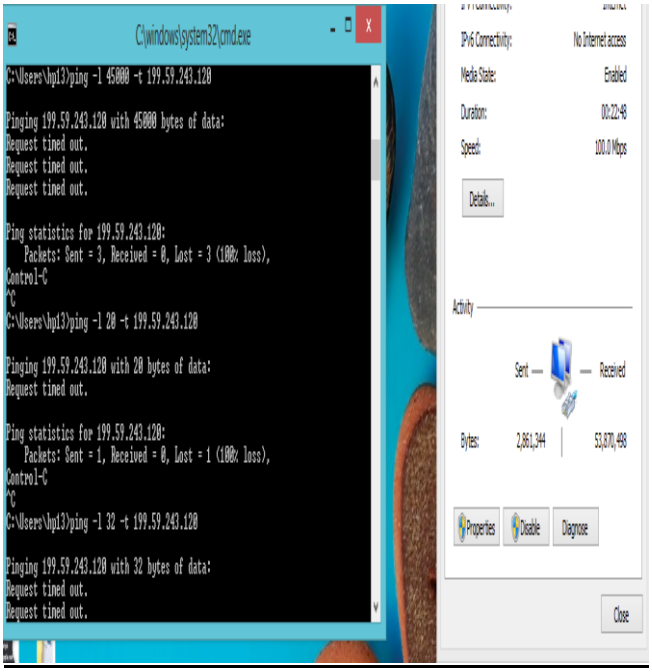


Fig. 9 Pinging a website

As per the survey when we manipulate the default packet size of different site the output is given in the below table i.e. table I.

In this table different companies with their IP address and manipulation of default packet size and notice the result after that manipulation.

Company name	IP address	Default packet size	Changed packet size	effect	Result
Oriental bank of Commerce	64.46.39.14		32 35500 bytes	sent=21 pkts; received pkts=21 pkts; loss=0%	vulnerable to DDoS
Isro.gov.in	220.220.21.137		32 1472 bytes	sent=10 pkts; received pkts=10 pkts; loss=0%	not vulnerable
Pakistanarmy.gov.pk	104.16.58.155		32 35499 bytes	sent=20 pkts; received=20 pkts; loss=0%	vulnerable to DDoS
Google.com			32 1200 bytes	sent=10 pkts; received=10 pkts; loss=0%	not vulnerable
Cisco.com	72.163.4.161		32 650 bytes	sent=7, received=1, lost=6 [85%]	not vulnerable
Sap.com	155.56.47.116		32 66 bytes	RTO	not vulnerable
Smartprix.com	199.59.243.120		32 54 bytes	RTO	not vulnerable

I.

TABLE SHOWS WHICH SITES ARE MOST VULNERABLE TO DDOS

According to the table Oriental bank of commerce is most vulnerable to DDoS attack, the maximum packet size allowed is 35500 bytes. Sap and Smart prix has disabled there ICMP Packets, In case of big companies as we increase the size of packet then loss % increases.

At next level we have to find the Hops between source and destination

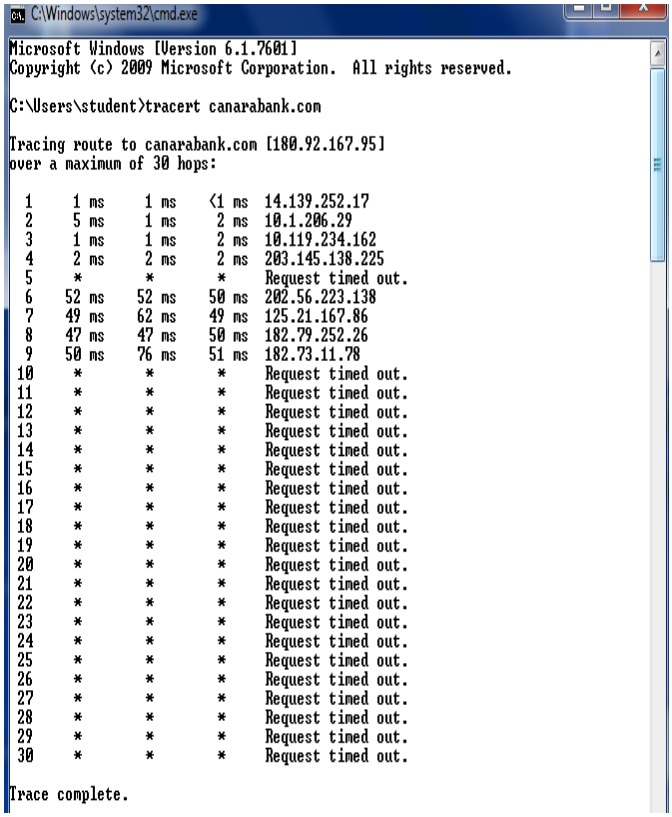


Fig. 10 hops between source and destination

V. RESULT

Company name	IP Address	TTL	packet size	maximum reponse time	Min response time	Average response time	Loss%
Cisco	72.163.4.161	235	32 bytes	281ms	278ms	279ms	0
Sap	155.56.47.116	RTO	RTO	RTO	RTO	RTO	RTO
Smartprix	199.59.243.120	51	32 bytes	190 ms	164ms	171ms	0
Youtube	216.58.220.26	59	32 bytes	63ms	34ms	26ms	0
Dominos	205.218.22.49	RTO	RTO	RTO	RTO	RTO	RTO
Microsoft	23.100.122.175	RTO	RTO	RTO	RTO	RTO	RTO
Flipkart	163.53.78.58	56	32 bytes	66ms	61ms	64ms	0
Amazon	54.239.32.8	RTO	RTO	RTO	RTO	RTO	RTO
Coviam	192.165.226.173	50	32 bytes	303ms	296ms	299ms	25%
Bank Of India	107.162.134.151	242	32 bytes	323 ms	291 ms	303 ms	0
Oriental bank of commerce	464.46.39.14	49	32 bytes	382 ms	335ms	363ms	0
HDFC	104.16.215.253	55	32 bytes	4ms	3ms	3ms	0
SBI	210.210.1.179	RTO	RTO	RTO	RTO	RTO	RTO
ICICI Bank	182.79.247.30	Expired in transit	32 bytes	Nil	Nil	Nil	Nil
Axis bank	195.60.68.81	52	32 bytes	176 ms	175ms	175ms	0
Kotak mahindra	203.196.200.43	RTO	RTO	RTO	RTO	RTO	RTO
Indusind bank	78.41.204.29	53	32 Bytes	149ms	148ms	148ms	0
Bank Of Baroda	45.249.109.60	RTO	RTO	RTO	RTO	RTO	RTO
Eshiksha.com	141.8.225.237	239	32 bytes	291 ms	280ms	288ms	0
India Education	70.42.23.198	RTO	RTO	RTO	RTO	RTO	RTO
Scholastic	204.74.99.100	RTO	RTO	RTO	RTO	RTO	RTO
IndiaEdu	69.64.35.130	47	32 bytes	302	289	239	0
Room108	208.73.211.70	239	32Bytes	293ms	281ms	286ms	0
Britannica.com	38.69.47.81	49	32 Bytes	273 ms	272ms	272ms	0
Enchanted learning	192.41.222.81	51	32 bytes	354ms	308ms	329ms	0
ekidzee	202.46.202.44	RTO	RTO	RTO	RTO	RTO	RTO
Admission news	77.75.136.126	240	32 bytes	158ms	147ms	150ms	0
Drdo	202.159.220.134	RTO	RTO	RTO	RTO	RTO	RTO
Isro.gov.in	210.210.21.137	54	32 bytes	45ms	34ms	39ms	0
cdac	196.1.113.45	RTO	RTO	RTO	RTO	RTO	RTO
cdot	220.156.188.75	RTO	RTO	RTO	RTO	RTO	RTO
nasa.gov	52.0.14.116	RTO	RTO	RTO	RTO	RTO	RTO
Pakistan army	104.16.58.155	55	32 bytes	33ms	19ms	24ms	0
mofa.gov.pk	203.101.184.9	RTO	RTO	RTO	RTO	RTO	RTO
Google.com	216.58.220.206	59	32 bytes	25ms	3ms	9ms	0
yahoo.com	98.138.253.109	49	32 bytes	338ms	328ms	330ms	0
facebook.com	31.13.95.36	74	32 bytes	303ms	289ms	290ms	0
Rediff.com	180.149.59.155	61	32 bytes	6ms	3ms	4ms	0
Igdtuw.com		RTO	RTO	RTO	RTO	RTO	RTO
sedulitygroups.com		RTO	RTO	RTO	RTO	RTO	RTO
gmail,.com	216.58.220.197	59	32 bytes	6ms	3ms	4ms	0
Hotmail.com	157.56.172.28	230	32 bytes	265ms	259ms	262ms	0
upsc.gov.in	203.94.248.194	55	32 bytes	41ms	15ms	28ms	0
Yahoogames	98.137.236.150	49	32 bytes	310ms	293ms	298ms	0

II. TABLE OF ALL 50 SITES SURVEY

After the survey of 50 different website, thus it involves target IP address, Operating system used worldwide, Link speed, packet size, manipulated packet size and number of hops between source and destination. By this survey we can also find the number of websites that disables the ICMP packet. Website at which ICMP Packets are disabled, they do not reply for the ping command they just show RTO (Request Time Out), but we can find IP address of those websites. By using the IP address we can manipulate the packet size by using the utility**:** ping –l packet size –t IP address of target machine, here packet size can be 0-65,500 bytes. The default packet size in windows is 32 bytes.

VI. CONCLUSIONS

Thus ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. But now-a-days attacker uses ICMP packet for attack purpose. Attacker sends ping request to victim machine to check whether the victim machine is alive or not. If machine is alive, then reply back otherwise RTO. Attacker gathers many information from ping command i.e. Victim machine IP address, O.S, Default packet size. Attacker uses these parameters for DDoS attack. Attacker send the abnormal sequence of ICMP packets to the victim machine to choke it. The future scope is to propose an algorithm using the up given parameters for the ICMP flood DDOS Detection.

ACKNOWLEGMENT

This study is proposed by reviewing different research papers and after reviewing them we got new idea for detecting ICMP flood DDoS attack by exploring the new parameters.

REFRENCES

[1] [1]Sandeep, Ranjeet,A study measure of DOS & DDOS- Smurf Attack and Preventive measures, International Journal of Computer Science and Information Technology 2014

[2] Virendra Kumar yadav ,Munesh Chandra Trivedi, B.M Mehtre, DDA an approach to handle DDOS (Ping flood) Attack, Journal of Computer science 2014.

[3] Ankita Mangotra**,** Vivek Gupta, Review paper on DDoS, International Journal of Advances in Science and Technology (IJAST) Volume 2 Issue 3(September 2014).

[4] Samantaghavi Zargar, James Joshi, David Tipper, A Survey of Defence mechanism against DDOS Flooding Attacks, IEEE Communication survey 2013.

[5] Kartikey Agarwal, Dr. Sanjay Kumar Dubey, network Security: Attacks and Defence, International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.

[6] Shakti Arora, Arushi Bansal, Survey on prevention Methods on DDoS Attacks, International Journal of Advance Research in Computer Science and Software Engineering, Volume 4 Issue 7 July 2014.

[7] Khadijah Wan Mohd Ghazali and Rosilah Hassan Flooding Distributed Denial of Service Attacks-A Review, Journal of Computer Science 2011.

[8] M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.

[9] J.Udhayan, R.Anitha, Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with AttackProductivity Analysis, 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[10] J.Wang3, R.Phan, J.N.Whitley, .J.Parish,DDoS AttacksTraffic and Flash Crowds Traffic Simulation with aHardware Test Centre Platform.

[11] Neha Gupta, Ankur jain, DDOS Attack Algorithm using ICMP flood, International conference on computing for Sustainable global development.

[12] M.A. Vinoth kumar and R. Udaya kumar, Identifying and Blocking high and low rate DDOS ICMP Flooding, Indian Journal of science and technology, November2015.

[13] Neha Gupta, Ankur Jain, Pranav Saini, Vaibhav Gupta,DDoS Attack algorithm using ICMP Flood.

[14] Himanshi bajaj, Indu sibal, Dr. Anup Girdhar, Study of DoS/DDoS attack using ICMP protocol.Cyber Times International Journal of Technology and Management 2014.

[15] AKAMAI, 2015 "DDOS attack activity at a glance", [Accessed at 25 November 2016].