

Ping of death

Khandaker Mushfiqur Rahman

July 2019

1 Introduction

Ping of death is a type of network attack that can make the network congested by sending huge amount of traffic towards a particular IP address. Because the network is congested, it won't be able to serve legit users, thus a denial of service is going to be created. In late nineties, ping of death was particularly a dangerous attack because the identity of the user could have been easily spoofed. But in the midst of 1997, the operating system vendors had made patches available to avoid the ping of death. Still, many Web sites continue to block Internet Control Message Protocol (ICMP) ping messages at their firewalls to prevent any future variations of this kind of denial of service attack. So currently this attack is not that useful in practical attacks.

2 Definiton

Ping of death, also known as 'Long ICMP attack' is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes or sending IP packets of 65,536 repeatedly allowed by the IP protocol. The network ping tool was created by Mike Muuss in 1983. It contains almost one thousand lines of code and has become the standard packaged tool for various network applications and operating systems.

The ping utility works by generating an ICMP data unit that is then encapsulated into IP datagrams and transmitted over the network. After receiving the echo request, the destination node copies its payload, destroys the original packet and generates an echo reply with the same payload it received.

3 What is PING?

Ping is a network diagnostic tool used primarily to test the connectivity between two nodes or devices. To ping a destination node, an Internet Control Message Protocol (ICMP) echo request packet is sent to that node. If a connection is available, the destination node responds with an echo reply.

The ping utility works by generating an ICMP data unit that is then encapsulated into IP datagrams and transmitted over the network. After receiving the echo request, the destination node copies its payload, destroys the original packet and generates an echo reply with the same payload it received.

Ping calculates the round-trip time of the data packet's route from its source to the destination and back, and determines whether any packets were lost during the trip. Depending on the operating system, ping utility output varies. However, almost all ping outputs display the following:

- Destination IP address
- ICMP sequence number
- Time to live (TTL)

- Round-trip time
- Payload size
- The number of packets lost during transmission

The ping tool displays various error messages if a round trip is not completed successfully. They include the following:

TTL Expired in Transit: Determines the maximum amount of time an IP packet may live over the network before being discarded if it has not reached its destination. To address this error, try to increase TTL value by using the ping -i switch.

Destination Host Unreachable:

Indicates that the destination node is down or is not operating on the network. It may even occur due to the non-existence of a local or remote route for the destination host. To address this error, modify the local route table or switch the node on.

Request Timed Out:

Indicates that the ping command timed out because there was no reply from the host. It indicates that no echo reply messages were received due to network traffic, failure of Address Resolution Protocol (ARP) request packet filtering or a router error. Increasing the wait time using the ping -w switch may address this problem.

Unknown Host:

Indicates that the IP address or the host name does not exist in the network or that the destination host name cannot be resolved. To address this issue, verify the name and availability of the domain name system (DNS) servers.

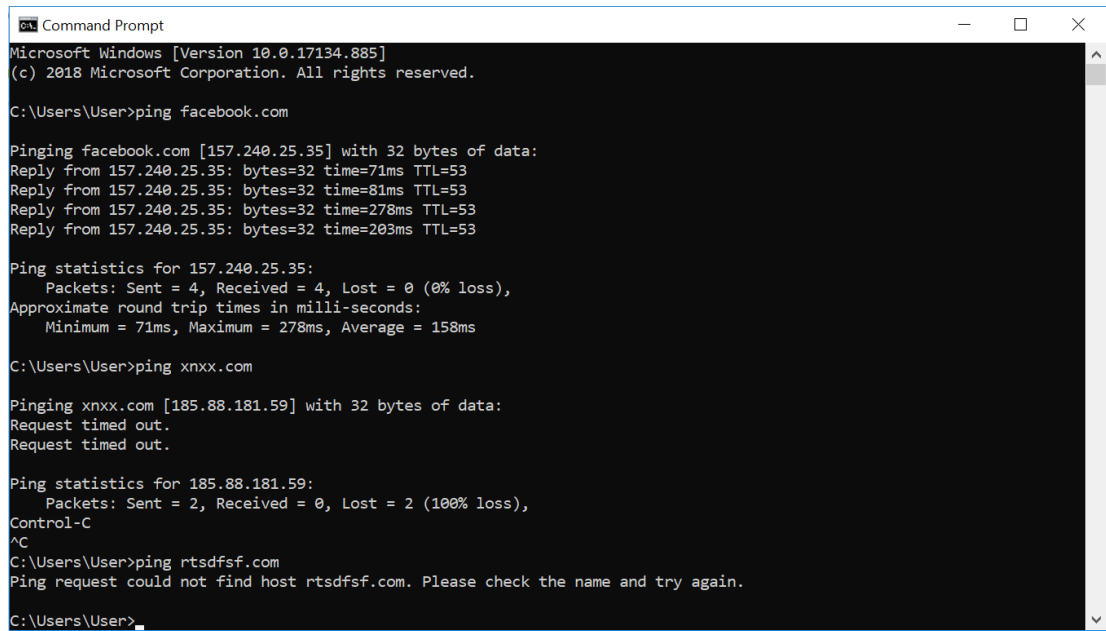
4 Implementing normal PING in our device

Implementing ping in our day to day devices is easy. Just simply type "cmd" in your search bar and you will find 'command prompt'. In the command prompt, write commands with structure,

```
$ ping "website-name"
or
$ ping "ip-address"
```

for example:

```
$ ping "facebook.com"
or
$ ping "157.100.98.123"
```



```
Command Prompt
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\User>ping facebook.com

Pinging facebook.com [157.240.25.35] with 32 bytes of data:
Reply from 157.240.25.35: bytes=32 time=71ms TTL=53
Reply from 157.240.25.35: bytes=32 time=81ms TTL=53
Reply from 157.240.25.35: bytes=32 time=278ms TTL=53
Reply from 157.240.25.35: bytes=32 time=203ms TTL=53

Ping statistics for 157.240.25.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 71ms, Maximum = 278ms, Average = 158ms

C:\Users\User>ping xnxx.com

Pinging xnxx.com [185.88.181.59] with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 185.88.181.59:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\User>ping rtsdfsf.com
Ping request could not find host rtsdfsf.com. Please check the name and try again.

C:\Users\User>
```

Figure 1: A screen shot of ping.

Here, we have tried to ping facebook.com and ping successfully returned its IP address, TTL, time and its byte size.

Then we tried to ping a illegal website that is currently blocked in Bangladesh. Here, we are getting "request timed out" all the time.

finally we tried to ping a website address that doesn't exist! here we are getting the reply that ping could not find the website.

5 Attack Design

DOS attacks are illegal on networks that we are not authorized to do so. This is why we will need to setup our own network for this exercise. We will make our own LAN using seedlabs Virtual machine. We will switch to the computer that we want to use for the attack and open the command prompt. We will ping our victim computer with infinite data packets of 65500. This might not have heavy impact on the victim device. So we will also try to change the header and send malicious packets larger than 110,000 bytes wrapped in a ping message. But if we use Linux operating system instead of windows, then we might use some other way to demonstrate this network congestion.

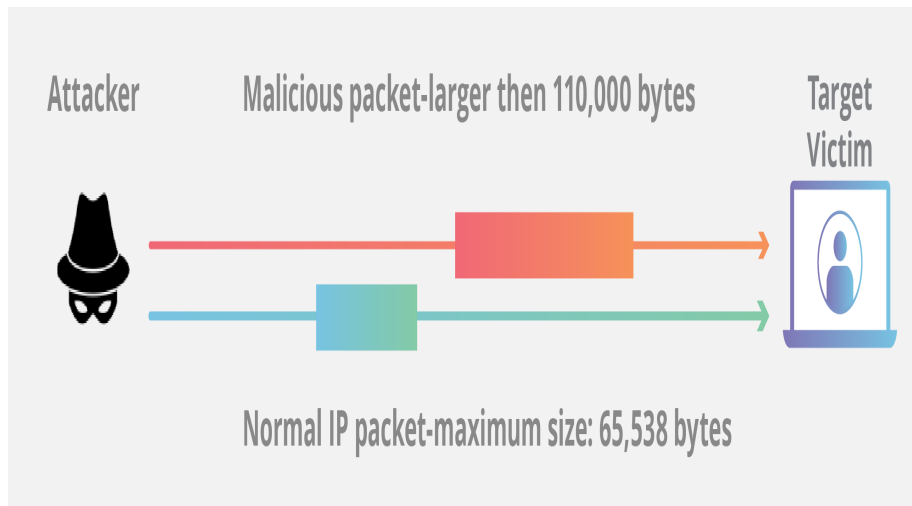


Figure 2: Network topology of Ping of death

We expect to see a result like this. If the attack is successful, then the network of the victim device should be congested. We will try to see this using the taskbar and go to networks. We should see something like this:

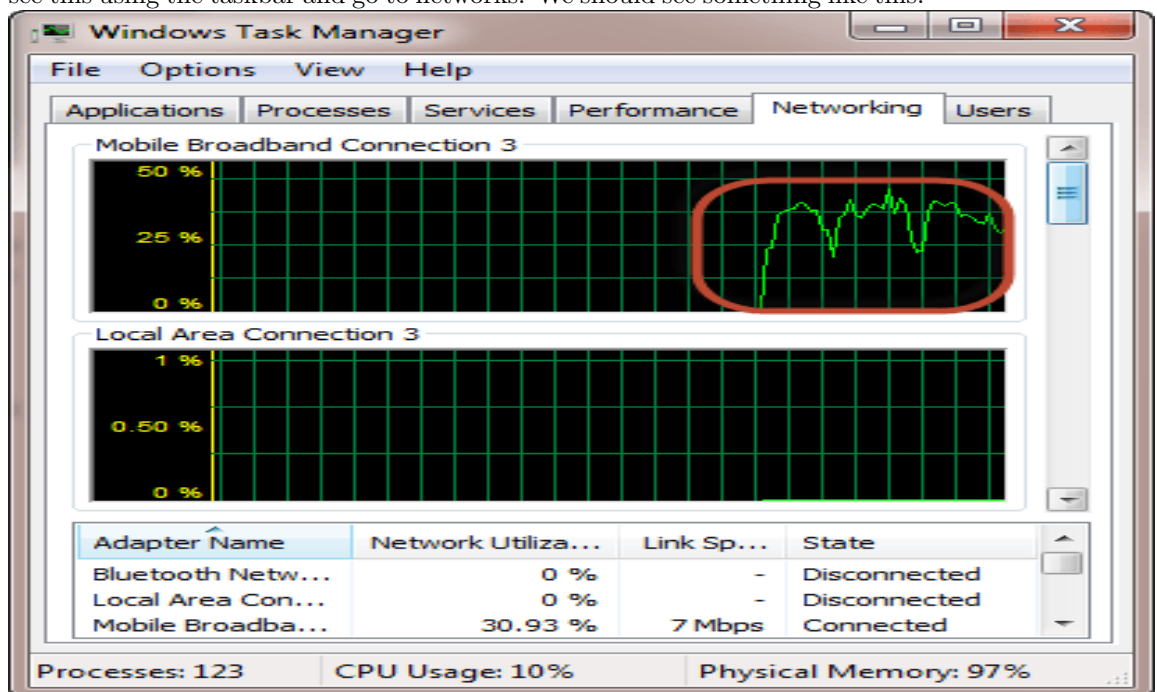


Figure 3: Network congestion demonstration

6 Network topology

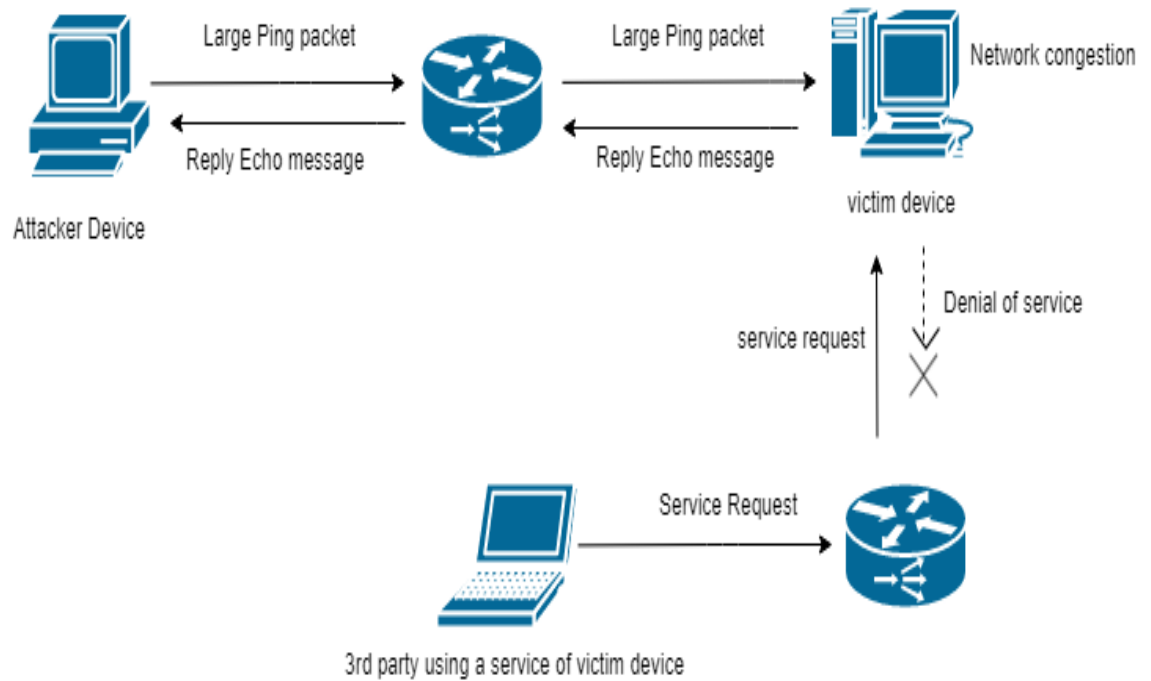


Figure 4: Network topology of Ping of death

7 Timing Diagram

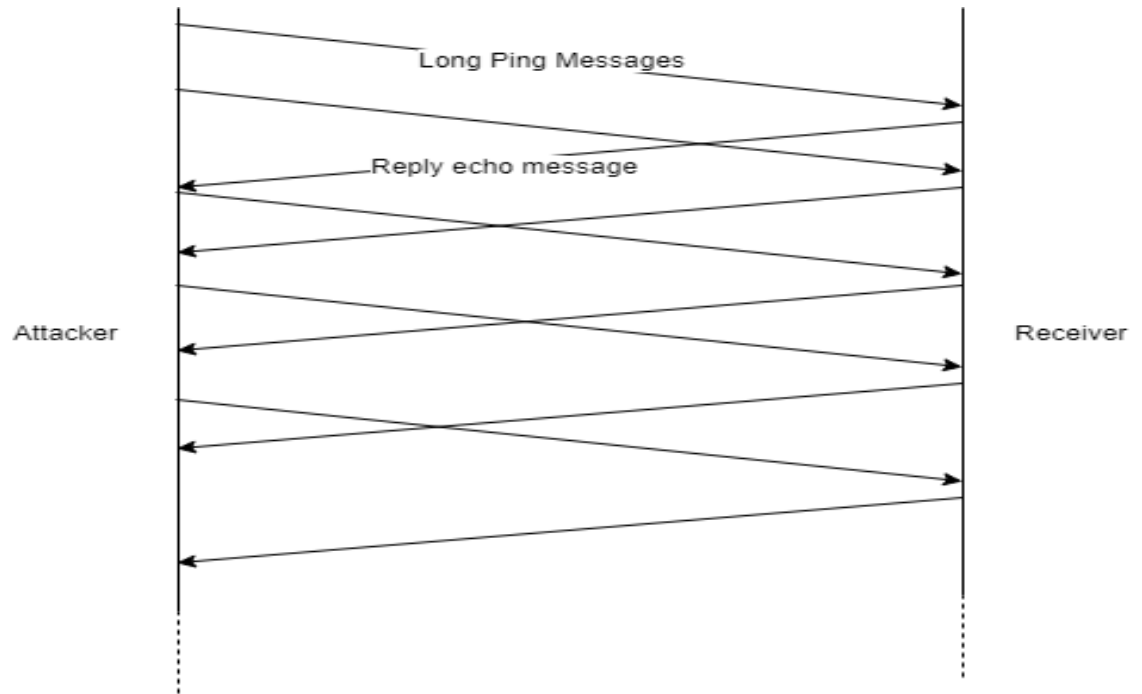


Figure 5: Timing diagram of Ping of death

8 Packet and Header of Ping

The ICMP header starts after the IPv4 header and is identified by IP protocol number '1'. All ICMP packets have an 8-byte header and variable-sized data section. The first 4 bytes of the header have fixed format, while the last 4 bytes depend on the type/code of that ICMP packet. These packets are then added with IP header and MAC header and send via network to reach and check the availability of its destination node. We will set the fragment offset of the header to send data packets larger than the normal limit.

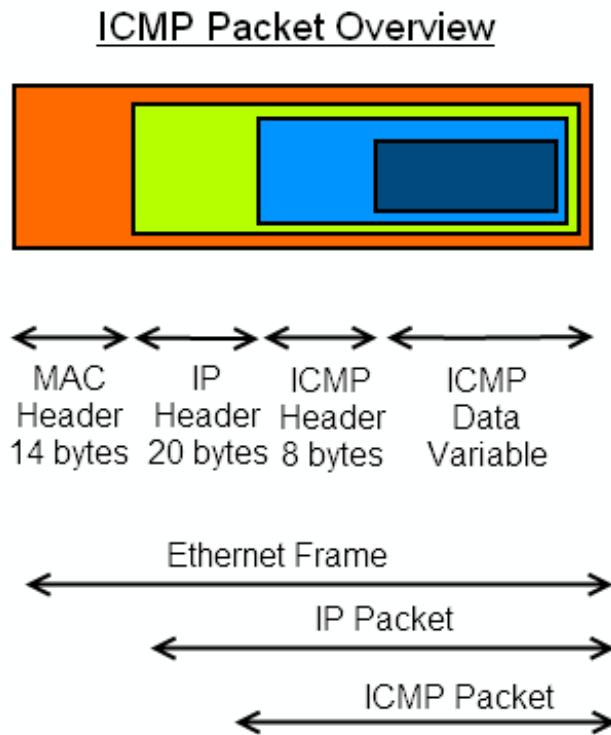


Figure 6: A screen shot of ping.

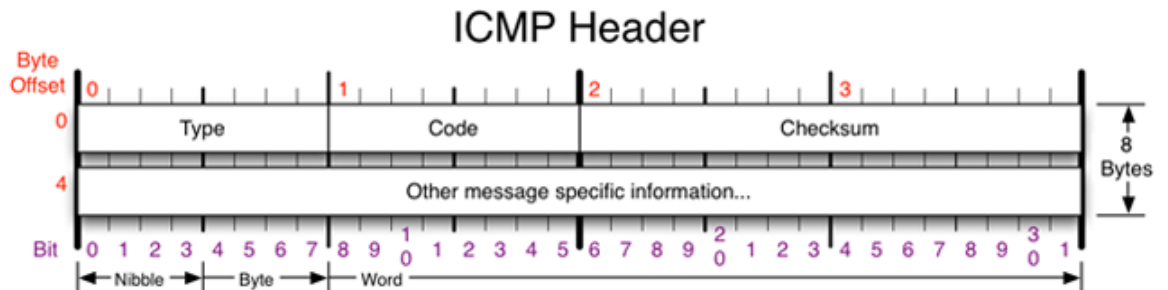


Figure 7: A screen shot of ping.

9 Justification

This attack should work on a controlled environment of a LAN in virtual machine. Because a ping of death attack sends huge amount of packets towards the victim and thus the victim becomes over occupied and its network becomes congested. so it can't deal with new requests. However, most of the modern oper-

ating systems use firewalls that can easily block any large size packets of ping.
So this attack will not work in a WAN or accross different networks.