Ping Of Death Attack

Contents:

- **Denial Of Service Attacks**
- **Ping Of Death Attack**
- **How Ping Of Death works ?**
- **Vulnerable Operatin systems**
- **How to Prevent Ping Of Death ?**

Deanil Of Service Attack (DOS)

What is Dos attacks and it’s types

What is DOS Attack ?

- DOS Attack is a malicious attemt by a single person or group of people to cause the victim, site or node to deny service to it customers.

- It’s purpose is shut down a site, not penetrate it.

Types of DOS Attacks :

- **DOS** = when a single host attacks
- **DDOS** = when multiple hosts attack simulatenously

What is Ping Of Death Attack ?

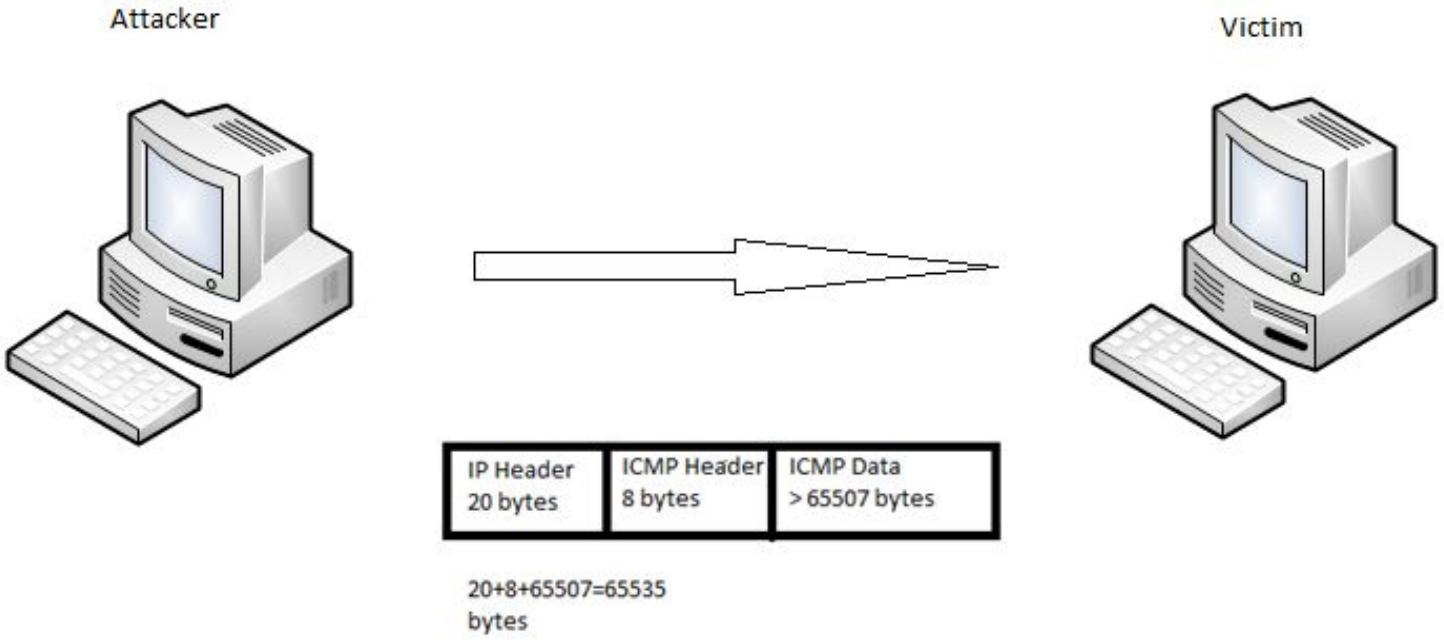
- Ping of Death is a type of **DOS** attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

- Ping of death attacks use the **Internet Control Message Protocol** (ICMP), but in theory other IP-based protocols could be used as well. Since modern systems are secured against the ping of death, today's malicious hackers tend to use a **ping flood** for attacks

How Ping Of Death works ?

- bug was discovered in the TCP/IP framework of many operating systems in the mid **1990s**, where sending a large packet (greater than the maximum allowable size of **65,535 bytes**) to a target machine would result in it becoming severely unstable, **crashing**, or **rebooting** it.

- This attack was made possible because such a large packet had to be reassembled on the receiving machine. When packet fragments were reassembled into a packet larger than the maximum allowable size of 65,535 bytes on the target machine, a buffer overflow occurred, causing instability, crashing or rebooting of the targeted machine.


Attacker
Victim
IP Header
20 bytes
ICMP Header
8 bytes
ICMP Data
> 65507 bytes
20+8+65507=65535
bytes

Operating systems Vulnerable to POD :

- This attack was first introduced in **1996** and it terrorized the world for about an year.By the end of **1997**, operating system vendors had made patches available to avoid the ping of death.

- **windows 95** was the last windows system that was vulnerable to this attack and **linux 2.0.23** was the last linux system to be vulnerable to this attack.

- **How to Prevent Ping Of Death ?**

- One solution to stop an attack is to add **checks to the reassembly** process to make sure the maximum packet size constraint will not be exceeded after packet recombination. Another solution is to **create a memory buffer** with enough space to handle packets which exceed the guideline maximum.

- The original Ping of Death attack has mostly gone the way of the dinosaurs; devices created after **1998** are generally protected against this type of attack

THANKS!

Any questions?

You can find me at

Amir Mansurian : Amir.m.mansurian@gmail.com

All documentation and codes are available at :

github.com/AmirMansurian/PingOfDeath-Attack

Spring 1400