**DoS: Ping of Death Attack**

The attacker tries to crash a remote system by sending a single ICMP IP packet. They are historical. Any operating system after 1998 are patched with this attack. This attack is not actually focused on ICMP but just a general attack using a bigger packet than the permitted size.

**Working:**

1. The attacker creates an ICMP echo request (PING). Ping packets are small in size and used to get the status of the remote system. Most system accepts and responds to ping requests. Ping packets can be 65,536 bytes in length and it contains IP Header, IP Options and the Data.
2. The attacker will create an IP packet that is bigger than 65,536 in length by using the technique called as fragmentation. The packet is fragmented into multiple pieces which contains the offset (Fragment ID) and the data.
3. The receiving system reconstructs the pieces by joining them using the offset. As the packet is bigger than 65,536 bytes the memory buffer of the receiving system will overflow and this causes the system to crash or reboot or freeze.

**Solution:**

This attack can be prevented by just adding more checks when reconstructing the fragmented pieces. Just by checking the offset and the length of the packet before reconstruction can help prevent the attack.

**ICMP Echo Request Ping**

**Target System**

**Header**

**Data**

**Options**

**Data**

**Packet Reassembly**

**Data Fragmentation**

**Dos: TCP SYN Flooding**

TCP/IP is the protocol used for communication between two systems. The communication takes place by a 3-way handshake. The 3-way handshake takes place in the following way. Consider a client and server wants to communicate.

1. The client sends a message to the server requesting for service and this message is called the SYN request. SYN stands for Synchronized.
2. The server responds back with a message called the SYN ACK where ACK stands for acknowledgement. This means the server received the request and is providing an opportunity for the client to connect with the server.
3. The client confirms the connection by sending an ACK back to the server and this establishes the connection between the client and the server.

This process is subject to an attack called as DoS: TCP SYN Flooding attack.

**Working:**

1. Whenever the server receives an SYN request from the client it has to allocate some space in the state-table for the request because the server has to provide resources to the client.
2. At this point we have a connection that is called a half open connection between the client and the server until the final ACK message is sent.
3. When the server receives multiple SYN request it will allocate multiple space in the state-table for the requests. But when the server does not receive the final ACK message from the client then that space allotted remains open for some period of time.
4. Usually, the SYN request contains the users IP address. But in case of an attacker, he will send a spoof IP address. There is no way for the server to know whether the client is legitimate.
5. So now when the state-table is filled up completely and the server receives a SYN request the server has no space to allocate so it does not send a SYN ACK back. In some cases, this may lead to crashing of the server. This leads to a legitimate user not being able to get the service.

**Server**

Half Open Connection

**Internet**

**Spoof IP**

**SYN (Synchronize)**

**Client**

**SYN-ACK (Acknowledgement)**

**ACK (Acknowledgement)**

**Dos: Smurf Attack**

It was created in the year 1998 and was designed to perform a Denial-of-Service attack on a targeted system. It takes advantage of the ICMP protocol. ICMP is used to get the status of the targeted system by pinging the system called the echo request. The targeted system will send a response known as the ICMP echo response.

**Working:**

It takes advantage of the ICMP (Internet Control Messaging Protocol) protocol. The protocol is used to get the status of a given machine with the help of the ping command. In older times, whenever an IP address received a ping request it broadcasts it to multiple systems. The Smurf attack takes advantage of this broadcasting process in order to attack a target system.

1. The attacker sends an Echo Ping Request to the broadcasting system by passing the targeted systems IP address.
2. The ICMP protocol generally doesn’t check for authenticity of the IP address sent in the request.
3. Once the broadcasting system receives the ping request it send the same request to multiple systems by passing the targeted systems IP address.
4. Now all the systems send the Echo Response to the targeted system all at once.
5. This overloads the targeted systems resources and completely block the system from responding to a legitimate user’s request.

**Target System**

**Ping Response**

**IP – 2.4.6.8**

**IP – 2.4.6.8**

**IP – 2.4.6.8**

**Broadcasting System**

**IP – 2.4.6.8**

**IP – 1.3.5.7**

**Attacker**