DOS Attack Methods

- Ping of death
- Land attack
- Teardrop
- Syn flood
- Smurf attack

Ping of Death

- A type of buffer overflow attack that exploits a design flaw in certain ICMP implementations where the assumption was that incoming packets would be small.
- IP does not allow single packets to exceed 65536 bytes, but the fragments themselves can add up to more than that.
- Attacker doesn’t need to know anything about the machine he is attacking, except for its IP address. .

  windows: ping –l 65527 –s 1 <hostname>.
- Target machine crashes,freezes or reboots.
- Most platforms now have effective patches and fixes, and the exploit is no longer as dangerous as it was.

Land Attack

- Exploits the *TCP* connection initiation process by sending a victim host a packet with identical source and destination address and port.
- Requires the ability to spoof packet source address.
- Requires the victim’s network to be unprotected against packets from coming outside with own IP address.
- The effects of the Land attack depends upon the *TCP* implementation, but range from temporary performance degradation to system crash.

Land Attack

- The attack can be divided into four stages:
  1. The attacker sends a spoofed connection request to the victim.
  2. The victim continues the three-way handshake by responding, and starts expecting ACK.
  3. However, as the source and destination information was the same, the victim receives the segment it sent in step 2. The received sequence number does not match the expected one, and the victim sends an ACK restating the sequence and acknowledgement number values it expects.
  4. The victim receives the ACK it just sent and seeing that the sequence number does not match the one expected it resends an ACK. The process repeats infinitely from step 4.

Packet Fragmentation

- If a router receives a packet that is too large for the next segment, it must divide the data into smaller pieces called **fragments** before sending it along.
- Each fragment uses the IP datagram format, but carries only a part of the data.
- Reassembly is performed at the distant end using two pieces of information.
    1. Offset field.
    2. Lenght field.

Offset Field

- Assume a packet of 8000 octets encouters a network link that can handle only 4000 octets.
- The router fragments the packet into two fragments, each 4000 octets long.
    - The first has a fragment offset of 0.
    - The second has a fragment offset of 4000.
- If the second fragment encounters a link where the MTU is 1000 octets, then it becomes four fragments, with offset field set to 4000, 5000,6000 and 7000.
- On the receiving end, the datagram is reassembled using the fragments and their offset values.
    - 0, 4000, 5000, 6000 and 7000.

Length Field

- Gives the length of the fragment and is used as a verification check to ensure there's no overlap and data was not corrupted in transfer.
- Example:
    - You place fragments 1 and 3 within a datagram.
    - You then try to place fragment 2, but find that it is too large and will overwrite some of the fragment 3.
    - You now know there is a problem, and can realign them or request that the data be resent if necessary.

Teardrop Attack

- Exploits the weakness of the IP protocol reassembly process.
- Uses the UDP protocol.
- Starts by sending a normal packet of data with a normal-size payload and a fragmentation offset of 0.
- Subsequent packets have modified fragmentation offset and field lengths.
- These malformed packets cause an unprotected system to crash, freeze or reboot.

Teardrop Attack

SYN Flooding

- Goes hand-in-hand with IP spoofing.
- Exploits the use of a small buffer space during the 3-way handshake to prevent a server from accepting inbound TCP connections.
- To establish a normal TCP connection:
    - The client sends a SYN packet to the server.
    - The server sends a SYN-ACK back to the client.
    - The client sends an ACK back to the server to complete the three-way handshake and establish the connection.

SYN Flooding

- The SYN attack.
  - The attack occurs by the attacker initiating a TCP connection to the server with a SYN. (Using a spoofed source address).
  - The server replies with a SYN-ACK.
  - ACK is never replied, causing the server to allocate memory for the pending connection and wait.
  - The half-open connections buffer on the victim server will eventually fill.
  - The system will be unable to accept any new incoming connections until the buffer is emptied out.

SYN Flooding

- There is a timeout associated with a pending connection, so the half-open connections will eventually expire.
- The attacking system can continue sending connection requests faster than the victim system can expire the pending connections.

Smurf Attack

- Utilizes IP spoofing and ICMP replies to flood the target host with packets.
- Broadcast address.
  - Special address that causes the underlying system to deliver a copy of a packet to all computers on a network.
- The attack phases:
  - The attacker sends a spoofed ping packet to the broadcast address of a network with a large number of hosts.
    - This network is called the amplifier or the bounce site.
  - Every host on the network receives the ICMP echo request and sends back an ICMP echo response, thus flooding the victime host.

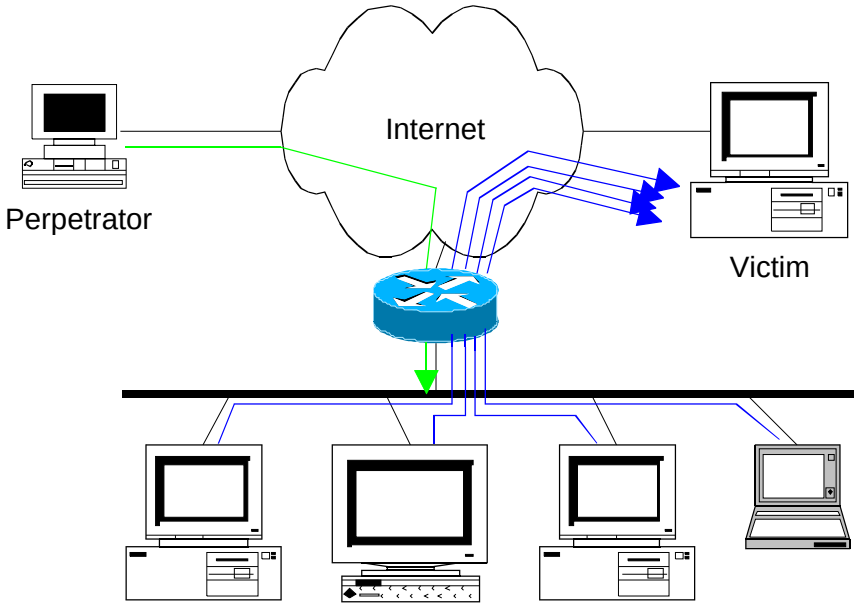
Smurf Attack

- Performance may be degraded such that beside the victim, also the amplifier networks become congested and unusable.
- Attack is easy to perform as attacker does not need fast connection. Example:
  - Attacker has a cable modem and sends a 1Mbps spoofed ICMP stream at the amplifier network, which has 150 hosts that respond. This yields a 150-Mbps attack traveling from the amplifiers toward the victim.

Smurf Attack

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply



Useful Links

- http://www.cert.org/tech_tips/denial_of_service.html
- http://www.denialinfo.com
- http://netsecurity.about.com