5.1.5 DoS Attack Facts

Denial of service (DoS) and Distributed denial of service (DDoS) attacks impact system availability by flooding the target system with traffic or requests or by exploiting a system or software flaw. The goal of a DoS attack is to make a service or device unavailable to respond to legitimate requests. Attackers may choose to overload the CPU, disk subsystem, memory, or network.

- In a DoS attack, a single attacker directs an attack against a single target, sending packets directly to the target.
- In a distributed DoS (DDoS) attack, multiple PCs attack a victim simultaneously. A series of computers scan target computers to find weaknesses and then compromise the most vulnerable systems. In a DDoS attack:
  - The attacker identifies one of the computers as the master (also known as zombie master or bot herder).
  - The master uses zombies/bots (compromised machines) to attack.
  - The master directs the zombies to attack the same target.
  - The attacker is able to effectively hide his identity by being two hops away from the victim.
- A distributed reflective denial of service (DRDoS) uses an amplification network to increase the severity of the attack. Packets are sent to the amplification network addressed as coming from the target. The amplification network responds back to the target system.

DoS attacks that use the ICMP protocol include:

ICMP Attack	Description
Ping Flood	A *ping flood* is a simple DoS attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. In a ping flood: ▪ The attack succeeds only if the attacker has more bandwidth than the victim. ▪ The attacker hopes that the victim will respond with ICMP Echo Reply packets, consuming outgoing bandwidth and incoming bandwidth.
Ping of Death	The *ping of death* (also called a long ICMP attack) is a DoS attack that uses the ping program to send oversized ICMP packets. In the ping of death: ▪ The attacker sends one or more very large ICMP packet (larger than 65,536 bytes) directly to the victim. ▪ The size of the packet causes the system to freeze, crash, or reboot.
Smurf	A *smurf* attack is a form of DRDoS attack that spoofs the source address in ICMP packets. A smurf attack requires an attacker system, an amplification network, and a victim computer or network. ▪ The attacker sends ICMP packets to an amplification network or broadcast address. The packets spoof the source address to be the target's. ▪ The amplification network responds by sending packets to the target (victim) site. ▪ The victim has thousands of replies to packets sent by the attacker. Many personal firewalls block all ICMP protocol messages in response to these attacks. The most effective protection measure the victim of a smurf attack can perform during an attack is to communicate with upstream providers. A simple phone call to request filtering on your behalf can weaken the effectiveness of a smurf attack.

DoS attacks that exploit the TCP protocol include:

TCP Attack	Description
SYN Flood	The *SYN flood* exploits the TCP three-way handshake as follows: ▪ The attacker floods a victim site with SYN packets. ▪ The victim responds to each SYN packet with a SYN ACK packet. ▪ The attacker does not respond with the last portion of the handshake (an ACK packet), leaving the victim waiting for a response. ▪ The attacker continues to send the victim SYN frames with a spoofed address. ▪ The victim continues to attempt sessions with the attacker, allocating resources to accommodate each of these inbound session requests. So many resources are allocated that the victim cannot process a legitimate inbound request for a TCP/IP session. A variation of the SYN flood attack is a *half-open scan* attack, in which the attacker sends SYN packets designed for certain ports. This is a form of port scanning also known as half-open scanning. The attacker doesn't send enough packets to cause a denial of service, but is able to determine the victim's open ports.
LAND	A LAND attack is one in which the attacker floods the victim's system with packets that have forged headers. In a LAND attack: ▪ The packets have the same source and destination address (the victim's). The packets also have the same source and destination port.

	▪ The victim's system has no procedure to deal with these packets. ▪ The victim's system holds the packets in RAM. ▪ As the victim's system continues to hold more and more packets in RAM, it is unable to process legitimate requests.
Christmas (Xmas) Tree	A Christmas (Xmas) tree attack (also known as a Christmas tree scan, nastygram, kamikaze, or lamp test segment) uses an IP packet with every option turned on for the protocol being used. Christmas tree packets can be used to conduct reconnaissance by scanning for open ports. They can also be used to execute a DoS attack if sent in large numbers. ▪ When sent to a target host, the TCP header of a Christmas tree packet has the flags FIN, URG and PSH set. By default, closed ports on the host are required to reply with a TCP connection rest flag (RST). Open ports must ignore the packets, informing the attacker which ports are open. ▪ Christmas tree packets require much more processing by network devices compared to typical packets. A DoS attack occurs if a large number of these packets are sent to the target host. ▪ Because Xmas tree scan packets do not have the SYN flag turned on, they can pass through firewalls and reach the target host.

DoS attacks that exploit the UDP protocol include:

UDP attacks	Description
Fraggle	A *fraggle* attack sends a large amount of UDP packets directed to broadcast addresses aimed at port 7 (echo) and port 19 (chargen--character generation) with spoofed source addresses. Fraggle is a variation of the smurf attack using UDP instead of ICMP to perpetrate an attack when firewall filters block ICMP messages.
Teardrop	A *teardrop* attack manipulates the UDP fragment number and location. In a teardrop attack: ▪ Fragmented UDP packets with overlapping offsets are sent. ▪ When the victim system rebuilds the packets, an invalid UDP packet is created, causing the system to crash or reboot.

In addition to specific automated attacks, *spamming* (sending unwanted email messages) can become a form of DoS attack because:

- It consumes bandwidth that is used by legitimate traffic.
- It can fill a mailbox or hard disk and result in legitimate email being rejected.
- Spam is often distributed by hijacking misconfigured SMTP servers.

Countermeasures for DoS and DDoS attacks include implementing:

- Intrusion detection systems (IDS) or intrusion protection systems (IPS).
- Strong anti-virus and anti-spyware software on all systems with internet connectivity.
- File and folder hashes on system files and folders to identify if they have been compromised.
- Reverse DNS lookup to verify the source address.
- External firewalls with the following filters:
  - Ingress filters that specify that any inbound frame must have a public IP address from outside of the organization's LAN.
  - Egress filters that specify that any outbound frame must have a private IP address within the organization's LAN.
  - Address filters to prevent traffic from specific attackers (if known).
- Filters to block unwanted traffic once a DoS attack begins. This helps to minimize the effects of the DoS attack. You can also contact your ISP to implement filtering closer to the source and reduce the bandwidth used by the attack.
- System patches and updates to remove flaws that are often exploited by DoS attacks.
