10.3.4 DoS Attack Type Facts

This lesson covers the following topics:

- DoS attack categories
- DoS and DDoS attack types
- DoS tools

DoS Attack Categories

There are four general categories of denial-of-service attacks. Although all DoS attacks involve an increase in traffic, an attacker may need to use one or more strategies to work around countermeasures that have been put in place.

Category	Description
Fragmentation attacks	Fragmentation attacks target a system's ability to reassemble fragmented packets. UDP and ICMP fragmentation attacks involve sending fake UDP or ICMP packets that are larger than the maximum transmission unit for the network. In order to accommodate this overage, the system disassembles the packets. Because these packets are fake and, therefore, cannot be reassembled, the target's resources are eaten up, and the server becomes unavailable.
Volumetric attacks	Volumetric attacks block traffic by taking up all available bandwidth between the target and the internet.
Amplification attacks	Amplification attacks exploit vulnerabilities in protocols and broadcast networks. The name is derived from the idea that the attacker uses intermediary computers and networks to amplify their attack's impact.
Application level attacks	Application-level attacks use all of the resources needed for an application to run, making it unavailable to other users.
Protocol attacks	Protocol attacks target the connection state tables of firewalls, load balancers, and application servers.

DoS and DDoS Attack Types

The following table lists the types of DoS attacks.

Attack	Description
TCP fragmentation	TCP fragmentation attacks, also known as Teardrop attacks, prevent TCP/IP packets from being reassembled. This is done by setting the flags on all frames to indicate that that they are fragments and providing instructions to connect to another frame that doesn't actually exist.
Ping flood	A ping is designed to test connectivity between two computers. Several commands are available to customize the ping command, making it a useful tool for network administrators. A ping flood attack is used to flood a target computer with large amounts of packets in an attempt to overload it. The default number of times a ping request is set is four. However, this can be changed using the –n command. The default size of a packet is usually around 64 bytes, but the –l command can request that additional data be sent for each packet. With a maximum of around 65,000 bytes, you can see how this traffic could add up very quickly.
Smurf attack	The Smurf attack is a DoS attack that targets ICMP protocol weaknesses, and has three steps. First, the attacker creates ICMP echo request packets using the spoofed IP address of the target machine. Then they send the packets to the broadcast address of a network, resulting in large number of devices sending the requested replies to the target's IP address. This attack's goal is to flood the target computer with traffic, making it difficult, if not impossible, to use.
Fraggle attack	A Fraggle attack is a DoS attack that targets UDP protocol weaknesses. A large number of UDP packets from a spoofed IP address are broadcast to a network in an attempt to flood the target computer.
Phlashing	Phlashing, also known as bricking, involves pushing incorrect updates to a system's firmware, causing irreversible damage, and rendering the computer about as useful as a brick.
SYN flood	A SYN Flood exploits the TCP three-way handshake. An attacker creates SYN packets with a non-existent source address. When the target machine responds with a SYN-ACK, it goes to the non-existent address, causing the target machine to wait for a response that it will never get.
Ping of death	The maximum size of a ping packet is 65,535 bytes. The TCP/IP rules do not allow for a ping over this max. However, a classic attack known as the ping of death circumvents this rule by fragmenting the packets. When they are reassembled, the packet size is too large, causing a buffer overflow and a system crash.
Land attacks	A land attack is a DoS attack that involves sending a modified SYN packet to a target. The packet is altered to reflect the host IP

address as both the destination and source IP address. As a result, the target machine replies to itself over and over.

DoS Tools

The following table lists DoS tools you can use.

Tool	Description
Trinoo	Trinoo, or trin00, is a set of programs that are used to for DDoS attacks. Trinoo uses UDP flooding to attack IP addresses.
Low Orbit Ion Cannon (LOIC)	A free and simple DoS attack tool.
DoSHTTP	DoSHTTP uses HTTP flooding to attack URLs. It can be run on any Windows system.
UDPFlood	The UDPFlood tool creates UDP packets for a network target.
Targa	Targa is a multi-functional tool that can perform land, WinNuke, and teardrop attacks.
Jolt2	Jolt2 is a DoS tool that sends numerous fragmented packets to a Windows machine.
Shark	Shark is a tool that is used to create botnets.
PlugBot	PlugBot is a tool that is used to create botnets.
Poison Ivy	Poison Ivy is used to create botnets.