**DoS Attack Facts**

A Denial of Service (Dos) attack prevents normal or legitimate activity by consuming resources or bandwidth. Resources can be consumed by flooding the target system with traffic or requests or by exploiting a system or software flaw. The following table describes three DoS types.

| **Attack Type** | **Characteristics** |
|---|---|
| Denial of Service (DoS) | An attacker sends packets directly to the end system.<br>A single attacker directed against a single target. |
| Distributed Denial of Service (DDoS) | Uses zombies to multiply the number of attackers.<br>Multiple attackers directed at the same target.<br>Allows the attacker to hide his identity. |
| Distributed Reflective Denial of Service (DRDos) | Uses an amplification network to increase the severity of the attack. |

The following table identifies several common forms of DoS attacks.

| **Attack Example** | **Characteristics** | **Countermeasures** |
|---|---|---|
| Smurf | Spoofs the source address in ICMP packets.<br>Sends ICMP packets to the amplification network (bounce site).<br>The bounce site responds to the victim site.<br>The victim has thousands of replies to messages he did not send. | Patch your systems.<br>Turn off broadcast functionality at border routers.<br>Deny spoofed internal packets.<br>Minimize ICMP traffic.<br>Deploy a network-based IDS.<br>Illicit ISP help.<br>Run a ping scanner, network mapping tool that employs ICMP packets, to test the connectivity of ports and IP addresses. |
| Fraggle | Similar to Smurf but uses UDP packets directed to port 7 (echo) and port 19 (chargen--character generation). | |
| Ping Flood | ICMP packets sent directly to the victim site. | |
| Ping-of-Death | One very large ICMP packet (larger than 65,536 bytes) sent directly to the victim site.<br>The size of the packet causes the OS to freeze, crash or reboot. Also known as Long ICMP attack. | |
| SYN Flood | Exploits the TCP three-way handshake.<br>1. The attacker sends an initial SYN packet.<br>2. The victim responds with a SYN ACK packet.<br>3. The attacker does not respond with the last portion of the handshake (an ACK packet), leaving the victim waiting for a response. | |
| Land | Spoofed SYN packets with the source and destination addresses identified as the victim site. This causes the system to crash as it attempts to respond to its own packet. | |
| Teardrop | Fragmented UDP packets sent with overlapping offsets.<br>When the victim system re-builds the packets, an invalid UDP packet is created, causing the system to crash or reboot. | |
| DNS Poisoning | Incorrect DNS data is introduced into a primary DNS server.<br>This redirects traffic to incorrect sites. | |

**Authentication Attack Facts**

*Authentication* is the process of proving and validating identity. After authentication, users have access to resources based on their identity. The following table lists common attacks directed at the authentication process.

| Attack | Characteristics | Countermeasures |
|---|---|---|
| Spoofing | Modified source and/or destination addresses in packets.<br>Used to hide the true source, or redirect traffic to another location.<br>Can include site spoofing that tricks users into revealing information. | Address filters<br>Prevent spoofed packets from crossing in to or out of your private secured network.<br>Ingress and egress filters are the most effective protection against IP packet spoofing. Ingress filters examine packets coming into the network, while egress filters examine packets going out of the network. These filters will examine packets based on rules to identify any spoofed packets. Any packet suspected of being spoofed on its way into or out of your network will be dropped.<br>Use certificates to prove identity.<br>Reverse DNS lookup can be used to detect spoofed e-mails because the indicated source e-mail address will often be invalid. Reverse DNS lookups perform a hostname-to-IP address lookup. Spoofed source e-mail addresses that are false will fail the reverse DNS lookup.<br>Use encrypted communication protocols, such as IPSec. |
| Man-in-the-Middle | Used to intercept information passing between two communication partners.<br>The third system (the attacker) is logically placed between the client and server. The client is fooled into authenticating to the attacker.<br>Both parties at the endpoints believe they are communicating directly with the other, while the attacker intercepts and/or modifies the data in transit. The attacker then authenticates to the server using the intercepted credentials.<br>Commonly used to steal credit cards, online bank credentials, as well as confidential personal and business information. | Use encrypted communication protocols, such as IPSec.<br>Use certificates<br>Perform mutual authentication<br>A Public Key Infrastructure (PKI) establishes mutual authentication through a third party trust model. This process allows the communicating parties to verify each other's identities through a trusted third party such as a Certificate Authority. |
| Replay | The attacker intercepts and records authentication traffic (an extension of a man-in-the-middle attack).<br>Captured packets are re-transmitted at a later time to establish a session. | Packet time stamps<br>Packet sequencing |
| Hijacking | Stealing an open and active communication session from a legitimate user (an extension of a man-in-the-middle attack).<br>The attacker takes over the session and cuts off the original source device.<br>The TCP/IP session state is manipulated so that a third party is able to insert alternate packets | IPSec or other encryption protocols<br>Certificate authentication<br>Mutual authentication<br>Randomizing sequencing mechanisms |

| | | |
|---|---|---|
| | into the communication stream.<br>Session hijacking has become difficult to accomplish due to the use of time stamps and randomized packet sequencing rules employed by modern operating systems. | |

**Software Attack Facts**

Malicious code (sometimes called *malware*) is software intended to cause harm. The best means to prevent a worm (or any other type of malicious code) from infecting a system or spreading from your system to others is system isolation. If there are no communication pathways into or out of a computer system, there is no means by which a worm or other malicious code can enter or leave. However, this is seldom possible.

Common malware examples are listed in the following table.

| Attack | Characteristics | Countermeasures |
|---|---|---|
| Virus | A program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found. Attaches itself to a host file or a hard drive sector.<br>Each time the host is used, the virus replicates.<br>Often focused on destruction or corruption of data.<br>Files with .doc, .exe, and .bat extensions can host viruses because they all have execution capabilities either via macros, directly, or via scripting.<br>Most often distributed via e-mail. Many viruses can e-mail themselves to everyone in your address book.<br>Examples: Stoned, Michelangelo, Melissa, I Love You. | Anti-virus software<br>User behavior modification and education<br>Block attachments at network borders<br>Prevent download of software from the Internet<br>Strict software installation policies<br>Remove removable drives to prevent unauthorized software entering a system |
| Worm | A program that can replicate and propagate itself.<br>Infects one system and spreads to other systems on the network.<br>A worm does not infect a master boot record like a virus, a worm does not require a host file or drive element.<br>Example: Code Red. | |
| Trojan Horse | Useful software such as utilities, screen savers, and games that hide malicious code.<br>Example: Back Orifice, NetBus, Whack-a-Mole. | |
| Logic Bomb | Malware that lies dormant until triggered.<br>A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity.<br>Logic bombs do not self-replicate. | |

Software exploitation involves taking advantage of known vulnerabilities in software and systems. For example, WinNuke is a software exploitation utility that affects Windows 98 and results in a TCP/IP stack failure. The following table lists common exploitation methods.

| Attack | Characteristics | Countermeasures |
|---|---|---|
| Back Door | An unprotected access method or pathway.<br>May be developer installed for easier debugging or | Auditing<br>Anti-virus and malware code scanning |

| | | |
|---|---|---|
| | to simplify distribution of software updates.<br>May be hacker installed. Any type of remote control tool or utility that grants unauthorized access.<br>On devices, it could be console ports, maintenance modems, or open connection ports. | For malicious user installed back doors, use access control management and controlled software deployment.<br>For developer installed back doors, disable them, change the defaults, or block access.<br>For device back doors, maintain physical access control. |
| Cross-site Scripting | Tricks a Web server into including malicious Hypertext Transfer Protocol (HTTP) code on a Web page. | Strict programming quality controls and development practices<br>Host-based intrusion detection system<br>File system encryption<br>Strict access controls<br>Program input validation checks<br>Auditing |
| Buffer Overflow | The operating system or an application does not properly set boundaries for how much and what type of data can be inputted.<br>Hackers submit data beyond what the system can handle.<br>The extra data executes in privileged mode. | |