Denial-of-Service (DoS)

Return to Glossary

A **Denial-of-Service (DoS)** attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them.

Restarting a system will usually fix an attack that crashes a server, but flooding attacks are more difficult to recover from. Recovering from a distributed DoS (DDoS) attack in which attack traffic comes from a large number of sources is even more difficult.

DoS and DDoS attacks often take advantage of vulnerabilities in networking protocols and how they handle network traffic. For example, an attacker might overwhelm the service by transmitting many packets to a vulnerable network service from different Internet Protocol (IP) addresses.

Source: https://searchsecurity.techtarget.com/definition/denial-of-service