DENIAL OF SERVICE

Denial of service (DoS) attacks are cyber-attacks that disrupt access to a network resource such as a website, email server, file system or networking device. The purpose of a DoS attack is to render the targeted resource unavailable for its intended legitimate use. This is usually accomplished by flooding the targeted resource with repeated requests for communication. These so-called “brute force” attacks overwhelm a computer’s ability to respond, making it unavailable for legitimate use.

Some DoS attacks are conducted using multiple computers directed at a single network resource. These are referred to as distributed denial of service (DDoS) attacks, and can involve hundreds or even thousands or remote computers.

TYPES OF DOS AND DDOS ATTACKS:

□ Consumption of resources. This type of DoS attack is directed at the computer or memory resources of a server and can consume all of the processing power, leaving it unable to handle legitimate requests.

□ Network “flooding” attack. Attacks of this type use large numbers of very basic network communication packets to consume all of the available bandwidth, effectively flooding the network with traffic.

□ Remote administration. In this type of threat an attacker is able to access the administration feature of a network device and either load corrupt firmware code, or otherwise cause the device to stop functioning.

□ Distributed denial of service (DDoS). This type of attack uses multiple compromised systems-sometimes hundreds or thousands- to send repeated requests for communication. DDoS attacks can involve computers on a company’s own network, and are usually caused by malware being unknowingly installed.

PROTECTING AGAINST DENIAL OF SERVICE ATTACKS:

□ Many network devices are able to detect denial of service attacks and to block repeated and unwanted communication requests. Proper configuration or network switches, routers and firewalls can limit the effectiveness of DoS attacks.

□ Intrusion detection and other intelligent hardware devices can identify network traffic and classify it as harmful or legitimate, blocking it or allowing it to pass.

□ Maintaining up-to-date and anti-malware software can help to detect and prevent a computer from being used in a DDoS attack.

□ If a company’s website or other services are being targeted, the network service provider can sometimes detect and block harmful traffic before it reaches its destination.