10.3.2 Denial of Service (DoS) Facts

A denial of service (DoS) attack occurs when a computer is used to flood a server with more packets than it can handle. Once a server is overloaded, the server becomes unavailable to other users and devices that are attempting to connect.

This lesson covers the following topics:

- DoS attacks
- DDoS attacks
- Damage of DoS and DDoS attacks
- Motivation for DoS and DDoS attacks

DoS Attacks

DoS attacks use a single connection to attack a single target. The attacker sends a large number of legitimate-looking requests to the server in a way that the server cannot determine which requests are valid and which are not. This barrage of requests overwhelms the system to the point that the server can't manage the capacity, resulting in the server being inaccessible by other users.

DDoS Attacks

The DoS attacks that you probably hear the most about are distributed denial of service attacks. These attacks use numerous computers and numerous internet connections across the world to overload the target systems. DDoS attacks are usually executed through a network of devices that the attacker has gained control of. The attacker uses compromised websites and emails to distribute specially designed malware to poorly secured devices. This malware provides an access point the attacker uses to gain control over the device at will. These zombie devices are recruited to cooperative teams called botnets. The attacker’s goal is to recruit as many zombie machines as possible, often creating botnets of thousands of computers. When an attacker is ready to strike, he will command his army of machines to launch a coordinated attack on a target system.

Damage of DoS and DDoS Attacks

DoS attacks can have a damaging impact on the victim. Many companies rely heavily, if not solely, on their web presence to operate their businesses. A targeted DoS attack will often result in slowed access, if not complete downtime for the victim’s web servers. Behind the scenes, a DoS attack can take down servers, databases, or other infrastructure critical to daily operations. For a business, the most painful impact can be the loss of revenue and the potential loss of customers. Depending on the size of the company, a DoS attack could result in thousands if not millions of dollars of lost revenue.

Motivation for DoS and DDoS Attacks

DoS and DDoS attacks do not provide the attacker with access to a resource. Instead, they prevent an authorized user from obtaining access to information or services. So, if the attacker doesn’t get access to the network, why would they even bother with a denial-of-service attack? There are several reasons:

Motivation	Description
Distraction	If the network team is distracted by a denial-of-service attack, there may be an opportunity for an attacker to infiltrate the network, download sensitive data, or cause damage without being noticed right away.
Damage reputation	Whether for revenge or competition, an attacker may want to embarrass the victim or tarnish their reputation.
Hacktivism	DDoS attacks are commonly used politically or morally driven hacktivists who want to stop the flow of information from a target website.
Fun	Sometimes hackers execute attacks for fun or out of boredom.
Profit	Attackers frequently try to exploit their victims for money. Their goal is to hold a network or web server hostage. Once-the-denial of service attack has been successfully implemented, the attackers request a ransom to stop the attack. DDoS services and botnets are available for rent at an hourly or daily rate.