Denial of Service (DoS)

- What is DoS & DDoS
- Methods Attacks
- Problems & Cost
- Types of Attacks
  - Three Way Handshake
- Way of infected
- Hacking Steps
- Avoid problems
- Defenses
- Example

A DoS (Denial of Service)

- Attack in which the primary goal is to deny the victim(s) access to a particular resource.
- A DoS (Denial of Service) attack aims at preventing, for legitimate users, authorized access to a system resource or the delaying of system operations and functions
- Is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers where the attack is aiming to cause the hosted web pages to be unavailable on the Internet.

Distributed Denial of Service (DDoS)

- In the summer of 1999, a new breed of attack has been developed called Distributed Denial of Service (DDoS) attack.
- Several educational and high capacity commercial sites have been affected by these Distributed Denial of Service attacks

What is DDoS?

- Attack uses multiple machines operating in concert to attack a network or site, and these attacks cause so much extra network traffic that it is difficult for legitimate traffic to reach your site while blocking the forged attacking packets.

- Attacker may use your computer to attack another computer, by taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses.

- The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

Methods of Attacks

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempt to disrupt a server by sending more requests than it can possibly handle, thereby preventing access to a service.
- attempts to prevent a particular individual from accessing a service.
- attempts to disrupt service to a specific system or person.

Methods of Attacks

A DoS attack can be perpetrated in a number of ways.There are three basic types of attack:

- consumption of computational resources, such as bandwidth, disk space, or CPU time.
- disruption of configuration information, such as routing information.

Methods of Attacks

- disruption of physical network components.
  - unusually slow network performance (opening files or accessing web sites)
  - unavailability of a particular web site
  - inability to access any web site
  - dramatic increase in the number of spam emails received

Scope of the problem

- A denial-of-service attack can effectively shut down a web site for hours or even days.
- DOS attacks cost significant losses
- On February 2000, several serious DDoS attacks targeted some of the largest Internet web sites, including Yahoo, Buy.com, Amazon, CNN and eBay.

Cost of DoS attacks for victim organizations

- Denial of Service is currently the most expensive computer crime for victim organizations: