Intrusion Detection,

Denial of Service (DoS)

Prepared By:Murad M. Ali
Supervised By: Dr. Lo'ai Tawalbeh

New York Institute of Technology (NYIT),
Amman's campus-2006

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

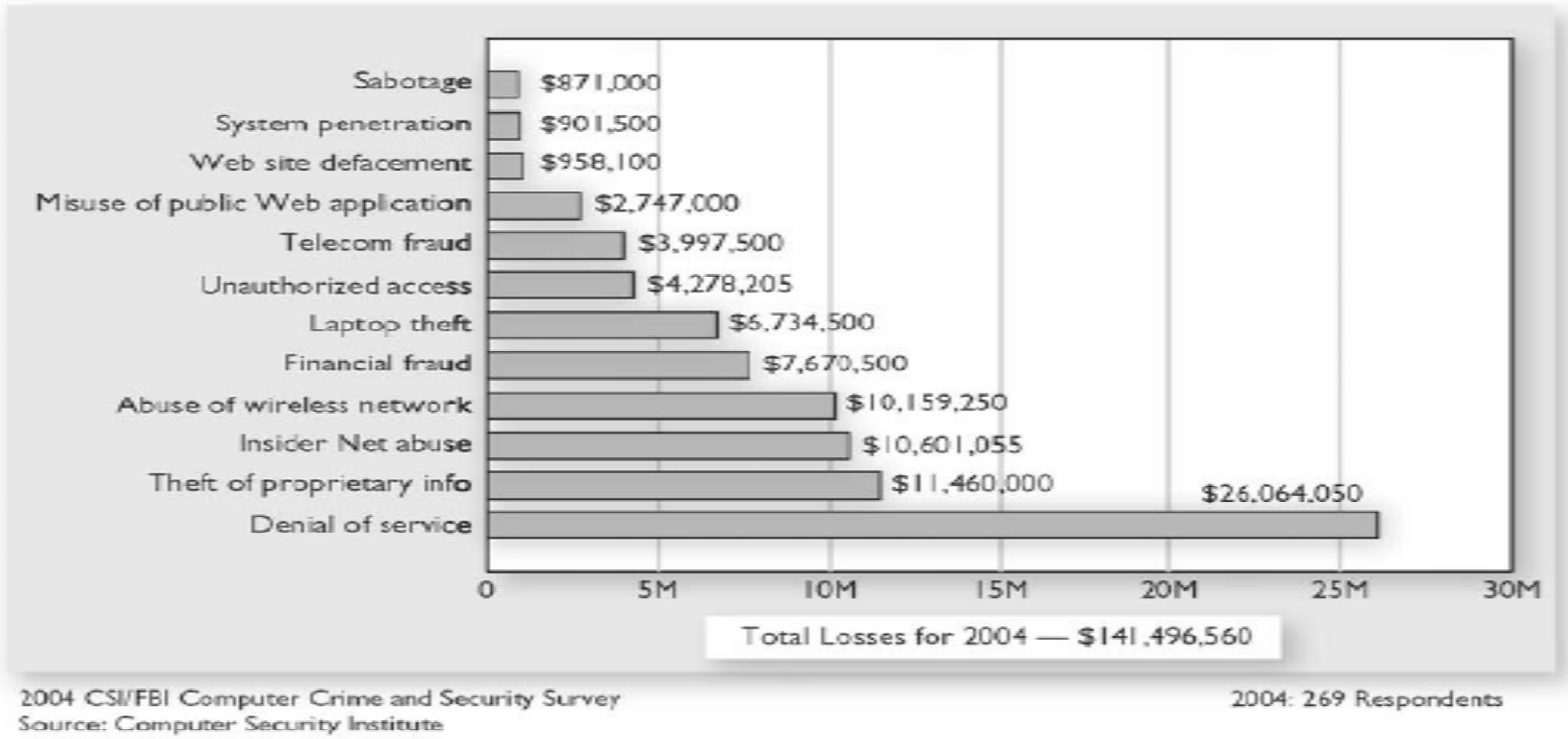
- disruption of physical network components.
  - unusually slow network performance (opening files or accessing web sites)
  - unavailability of a particular web site
  - inability to access any web site
  - dramatic increase in the number of spam emails received

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:



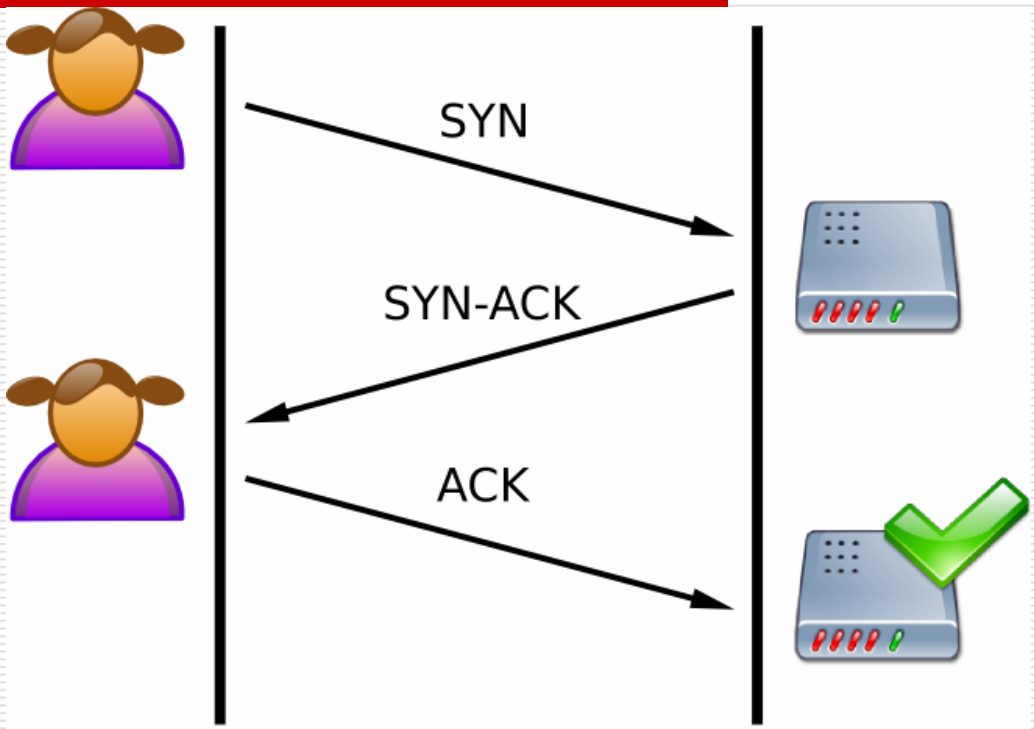
Types of Attacks

- SYN Flood
- Smurf Attack (ICMP Flood)
- LAND Attack
- UDB Flood
- Trinoo
- Tribal Flood Network (TFN &TFN2K)
- Stacheldraht

TCP Three Way Handshake

- When a computer wants to make a TCP/IP connection (the most common internet connection) to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer, sends a TCP/SYN packet which asks the server if it can connect. If the server will allow connections, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet detailing the specifics of its connection.

TCP Three Way handshake



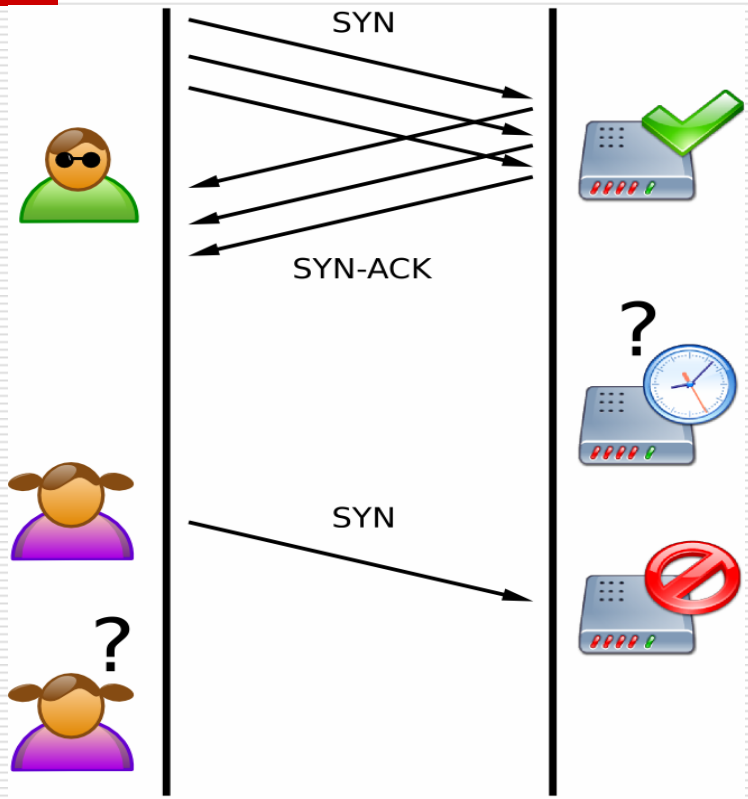
A normal connection between a user and a server. The three-way handshake is correctly performed.

SYN Flood

- Sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet, and waiting for an TCP/ACK packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections consume resources on the server and limit the number of connections the server is able to make, reducing the server's ability to respond to legitimate requests until after the attack ends.
- In a SYN flood the address of the client is often forged so that when the server sends the go-ahead back to the client, the message is never received because the client either doesn't exist or wasn't expecting the packet and subsequently ignores it. This leaves the server with a dead connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which keeps legitimate clients from making connections.

SYN Flood

The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and eat the server resources. A legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.



Example

- The classic example is that of a party. Only 50 people can be invited to a party, and invitations are available on a first-come first-serve basis. Fifty people send letters to request invitations, but the letters have false return addresses. The invitations are mailed to the return addresses of the request letters. Unfortunately all the return addresses provided were fake, so nobody receives the invitations. Now, when someone actually wants to come to the party (view the website), there are no invitations left because all the invitations (connections) have been reserved for those 50 people.

Smurf Attack (ICMP)

- Technique that takes advantage of the ICMP (Internet Control Message Protocol).
- Smurf is installed on a computer using a stolen account, and then continuously "pings" one or more networks of computers using a forged source address.
- It relies on mis-configured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim.

LAND Attack

- Involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address with an open port as both source and destination. The attack causes the targeted machine to reply to itself continuously and eventually crash.

User Datagram Protocol (UDP)

- UDP floods include "Fraggle attacks". In a fraggle attack an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. It is a simple rewrite of the smurf attack code.

Trinoo

- Is a complex DDoS tool that uses "master" programs to automate the control of any number of "agent" programs which launch the actual attack. The attacker connects to the computer hosting the master program, starts the master, and the master takes care of starting all of the agent programs based on a list of IP addresses. The agent programs then attack one or more targets by flooding the network with UDP packets. Prior to the attack, the perpetrator will have compromised the computer hosting the master programs and all the computers hosting the agent program in order to install the software.

Tribal flood Network (TFN)

- like Trinoo, uses a master program to communicate with attack agents located across multiple networks.
- TFN launches coordinated DoS Attacks that are especially difficult to counter as it can generate multiple types of attacks and it can generate packets with spoofed source IP addresses.
- Some of the attacks that can be launched by TFN include UDP flood, TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast

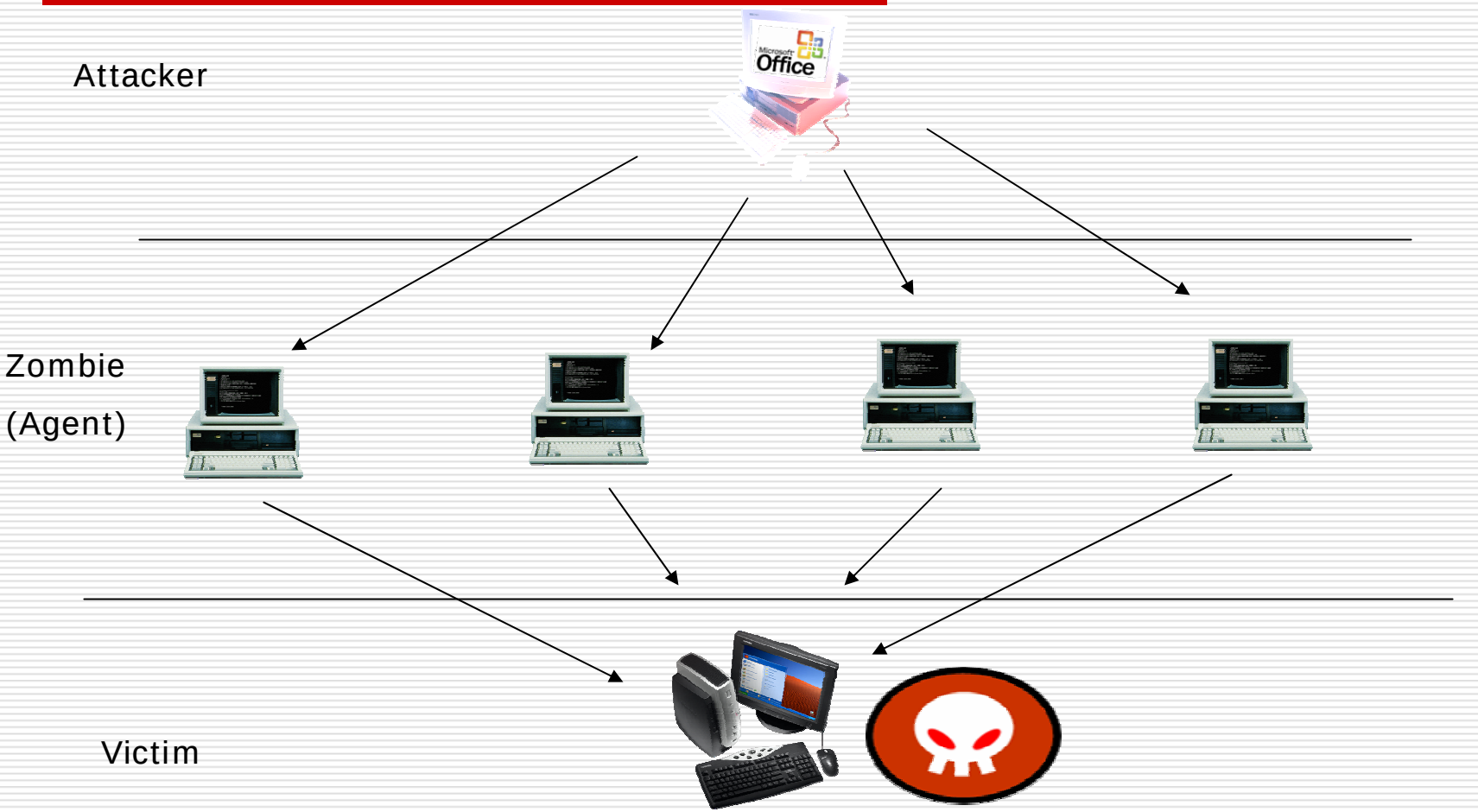
Stacheldraht

- Also based on the TFN and Trinoo client/server model where a master program communicates with potentially many thousands of agent programs.

- Stacheldraht adds the following new features:
  - encrypted communication between the attacker and the master program, as well as automated updates of the agent programs using rcp (remote copy).

- Stacheldraht launches coordinated DoS Attacks that are especially difficult to counter as it can generate multiple types of attacks and it can generate packets with spoofed source IP addresses. Some of the attacks that can be launched by Stacheldraht include UDP flood, TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast.

Zombie Network



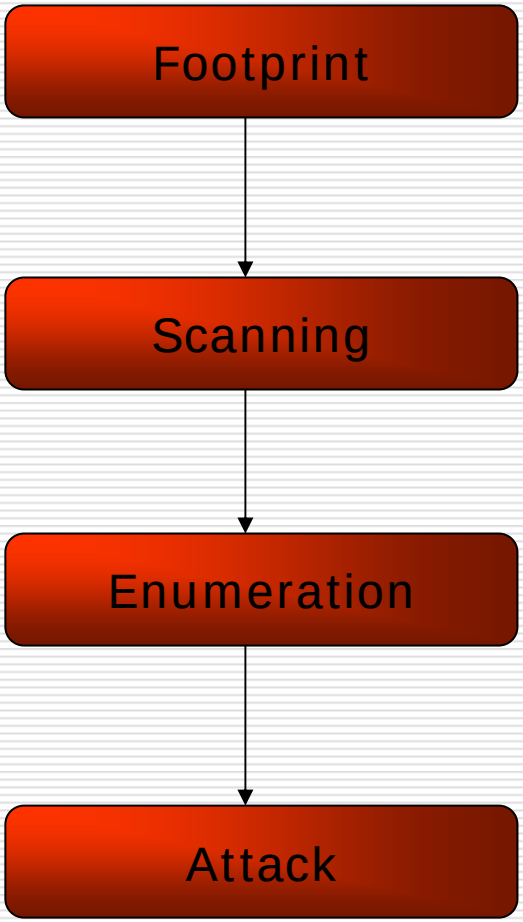
Way of Infected

- Malware can carry DDoS attack mechanisms; one of the more well known examples of this was MyDoom.
- Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.
- A system may also be compromised with a trojan, allowing the attacker to download a zombie agent (or the trojan may contain one).
- Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts.

MyDoom(Compter Worm)

- Also known as **W32.MyDoom@mm**, **Novarg**, **Mimail.R** and **Shimgapi**, is a computer worm affecting Microsoft Windows. It was first sighted on January 26, 2004. It became the fastest spreading e-mail worm ever (as of January 2004).
- Appears to have been commissioned by e-mail spammers so as to send junk e-mail through infected computers. The worm contains the text message *"andy; I'm just doing my job, nothing personal, sorry,"* leading many to believe that the worm's creator was paid to create it. Early on, several security firms published their belief that the worm originated from a professional underground programmer in Russia.

Hacking Steps



- Range of Target address
- Collection of Information
- Trace Path

- ascertain all service which is listening on a large scale

- Enumerate user's name
- version of Software

- DDoS
- Other Attcker

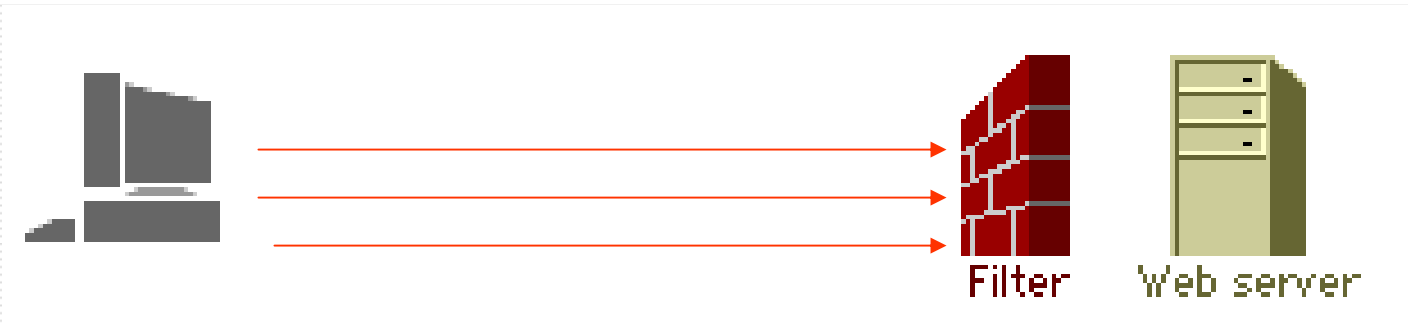
Avoiding The Problem

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and filter.
- Updating the operating system.

Block the DoS Attacks

- One of the more common methods of blocking a "denial of service" attack is to set up a filter, or "sniffer," on a network before a stream of information reaches a site's Web servers. The filter can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed to block messages containing that pattern, protecting the Web servers from having their lines tied up.



Block the DoS Attacks

- Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data through. They are especially important for users who rely on "always on" connections such as cable or DSL modems.

Defenses

- Disable and filter out echo services
- Disable and filter out all unused UDP services.
- Good practice is to block all UDP ports below 900 (excluding some specific ports like DNS)
- Network administrators should log all information on packets that are dropped
- If you are providing external UDP services, monitor them for signs of misuse

Defenses

- Routers, machines, and all other Internet accessible equipment should be periodically checked to verify that all security patches have been installed.

- System should be checked periodically for presence of malicious software (Trojan horses, viruses, worms, root-kits, back doors, etc.).

Famous Example

- A 15-year-old script kiddie called Mafiaboy was arrested in an upper class neighborhood in Montreal in 2000. Using downloaded DoS attacks, he struck famous websites such as Yahoo, Dell, Inc., eBay, and CNN, causing roughly 1.7 billion dollars worth of damage. He pled guilty to 55 criminal charges and served 8 months in a youth detention center.
- Jeffrey Lee Parson was an 18-year-old high school student from Minnesota responsible for using the B Variant of the infamous Blaster worm. The program was part of a DoS attack against computers using the Microsoft Windows operating system. The attack took the form of a SYN flood which caused only minimal damage. He was sentenced to 18 months in prison in 2005.

Conclusion

- Several examples of large scale DoS attacks (yahoo, eBuy, CERT, FBI, Amazon).
- Increased number of consumers with high bandwidth technologies, but with poor knowledge of network security.
- Easy accessible, easy to use DoS attack tools.
- No final solution for attacks.


Thank You
Thank You