Denial of Service

Definition

• Denial of Service (DoS) is an attempt to make a computer’s resource unavailable to its intended users
• Distributed Denial of Service (DDoS) is an attack involving a large number of computers
• “Crashing” the computer to keep others from using it

Resources and Credits

• Information on Denial of Service attacks can be found on Wikipedia.
  – Graphics and some text in these slides was taken from the Wikipedia site
• The textbook discusses denial of service in several locations
• There are many websites with information on denial of service

Symptoms

CERT defines symptoms of denial-of-service attacks to include:
• 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—(an e-mail bomb)
**Ways to Generate a DoS Attack**

- Consumption of a resource (CPU, network bandwidth, file space, etc.)
- Causing a application to fail (stack overflow, integer overflow, etc.)
- Malicious change in configuration (i.e. routing tables)
- Disruption of the physical system (i.e. power, wiring, etc.)

**Ping**

- The ping network utility sends an ICMP echo packet to a remote computer. When received, the remote computer sends an ICMP echo-reply packet. This is very useful for checking network function and performance.
- There are special network addresses to broadcast a message to all computers

**Ping Flood**

- A ping flood attack broadcasts an ICMP echo packet to all computers on a network
- The return address of the packet is improperly set to the address of a victim computer
- All computers on the network send an ICMP echo-reply to the victim computer
- The large volume of packets can consume the victim’s network resources

**Ping Flood Mitigation**

- A computer should not accept an ICMP echo packet sent with a broadcast address
**TCP Connections**
- Establishing a TCP connection requires three messages.
- After the connection, the systems may exchange data.

**SYN Flood**
- An attacker can send many SYN packets to a victim.
- The attacker does not send an ACK.
- The half established connection consumes ports until the victim times out the attempt.
- Others may not be able to establish a connection.

**SYN Flood Mitigation**
- Decrease the timeout waiting for an ACK.
- Networks should filter packets with obvious incorrect source addresses.
- Minimize the amount of information saved from the SYN message.
- Increase the memory available to hold information about connections.

**Attacks on Poor Network Stacks**
- Some early implementations of TCP/IP were not created with security in mind.
- Errors in network packets could cause the software to fail:
  - Ping with larger than allowed packets
  - Mangled IP fragments with overlapping, over-sized payloads
  - Invalid value in the rarely used TCP urgent pointer.
**fork Bomb**

- If a programmer has access to a system, they may be able to run a program that starts and endless number of processes:
  ```c
  while (true) fork();
  ```
- This will create many processes consuming system resources, particularly PID numbers.
- The problem can be mitigated by limiting the number of processes a user can own.

**Userid Lock Out Attack**

- Some systems that request a userid and password will lock the account if they receive more than X bad passwords.
- If an attacker can get a list of users or enumerate the possible account numbers, they can send many invalid passwords locking out all users.
- Temporarily removing the lock out may open the system to other password attacks.

**Permanent Denial of Service Attacks**

- Permanent denial-of-service (PDoS or phlashing) changes a devices firmware.
- Rebooting or reloading the software will not correct the problem.
- Systems should be designed to carefully restrict how the firmware can be changed.

**Distributed Denial of Service Attack**

- Malware can infect a large number of computers to form a botnet that can be used in a DDoS attack.
- Many machines can generate more network traffic.
- Attacks from a widely distributed botnet can be hard to filter by a firewall.
DDOS Control

A botnet can be controlled in many ways:
• The attack mechanism, time and victim can be hard coded into the malware
• A control system can send messages to the botnet telling who to attack
• Attack code can be downloaded to the bots. This provides the most versatile attack mechanism

Unintentional DoS

• Sometimes a site may be overwhelmed by legitimate traffic
• An extremely popular website could post a prominent link to a second, less well-prepared site causing it to receive many requests
• The Universal Tube & Rollform Equipment Corporation’s website, utube.com, became heavily hit when youtube became popular

Firewall Defense

• Firewalls can be configured when an attack occurs to stop specific addresses
• DoS attack may use random return addresses
• DDoS attack may involve traffic from many locations
• A traffic bottleneck can occur in the network before the firewall

Intrusion Prevention Systems

• An intrusion prevention system can sometimes detect a signature or similarity in the attach packets