Denial-of-Service Attacks
Objectives

- Define a denial-of-service (DoS) attack
- Describe causes of DoS attacks
- Describe several varieties of DoS attacks
Objectives (continued)

• Define a distributed denial-of-service (DDoS) attack
• Discuss some known DoS and DDoS attacks
• Describe ways to prevent DoS and DDoS attacks
Causes of DoS Attacks

• Some major network defects and vulnerabilities
  – Vulnerability of the network architecture
  – Vulnerability of a specific server system architecture (Intel x86, AMD Opteron, etc.)
  – Defects and bugs in the operating system or software
  – Holes present within system security

• Some vulnerabilities cannot be closed by patching
  – Because there is an inherent bandwidth limit
Causes of DoS Attacks (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-up Modem</td>
<td>56 Kbps</td>
</tr>
<tr>
<td>ADSL</td>
<td>1.5 Mbps</td>
</tr>
<tr>
<td>Cable</td>
<td>3 to 6 Mbps</td>
</tr>
<tr>
<td>T-1/DS1</td>
<td>1.5 Mbps</td>
</tr>
<tr>
<td>T-3/DS3</td>
<td>1.5 Mbps</td>
</tr>
<tr>
<td>OC1</td>
<td>51.84 Mbps</td>
</tr>
<tr>
<td>OC3</td>
<td>155.52 Mbps</td>
</tr>
<tr>
<td>OC12</td>
<td>622.08 Mbps</td>
</tr>
<tr>
<td>OC24</td>
<td>1.244 Gbps</td>
</tr>
<tr>
<td>OC48</td>
<td>2.488 Gbps</td>
</tr>
<tr>
<td>OC192</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>OC256</td>
<td>13.271 Gbps</td>
</tr>
<tr>
<td>OC768</td>
<td>40 Gbps</td>
</tr>
</tbody>
</table>
Types of DoS Attacks

• See Figure 11-1
  – X axis = Flood attacks or software attacks
  – Y axis = Isolated attacks or distributed attacks
  – Z axis = Voluntary or involuntary, on the part of the systems administrator
Types of DoS Attacks (continued)

- *Preventable DoS*: It’s attack may occur when the system administrator has designed a network or application-level system to perform a variety of services.
- *Non-Preventable DoS*: it’s an attach which the system administrator could not have been expected to anticipate or prepare for.
Flood Attacks

• Consume the limited resources of a computer or a network
  – By transmitting a large number of packets as quickly as possible
• A flood attack can occur under the following conditions:
  – Sending connection requests
  – Consuming the bandwidth
  – Using your own resources
  – Consuming others’ resources
Flood Attacks (continued)

- Sending Connection Requests
  - Target or victim receives a large quantity of connection requests
  - Attacker is probably using a spoofed IP address
- Consuming Bandwidth
  - All of a network’s available bandwidth is consumed by sending a large number of packets
Figure 11-2  Connection request attack
Flood Attacks (continued)

• Using Your Own Resources
  – Hacker uses forged UDP packets to connect the echo service on one computer
    • To a service on another computer
  – Response for this packet will automatically be sent to the computer whose IP address the hacker is using
Figure 11-3  Echo request attack
Flood Attacks (continued)

- Consuming Other’s Resources
  - Hacker may be able to consume data structures
    - Simply writing a program or a script that replicates itself
  - Hackers also attempt to consume disk space
    - By using any feature that allows data to be written to a system’s hard disk
  - Hacker may be able to lock an account by executing a certain number of failed attempts to log in
Software Attacks

• Exploit the existing software weaknesses
• Effect is either degraded performance or crashes on the victim server
• Hackers generate a small number of carefully malformed packets to exploit known software bugs
  – Bugs allow hackers to change or damage configuration files
Software Attacks (continued)

• **Ping of Death**
  – A historical DoS attack in which the hacker uses the Ping utility to acquire access to a system
  – Hacker sends a packet larger than 64 KB to the target computer
  – Target system may crash or restart
  – Most legitimate Ping utilities do not allow you to send a ping of more than 64 KB
  – You can use Apsend to send an oversized packet
Software Attacks (continued)

Figure 11-4  Attempted Ping of Death
Software Attacks (continued)

• Ping of Death (continued)
  – You can block pings on your firewall
  – Almost all operating systems have been patched to deflect this attack

• DNS Service Attack
  – Domain Name Service (DNS)
    • Database that maps domain names to IP addresses
    – Two kinds of attacks are related to the DNS service: DNS spoofing and DNS overflow
Software Attacks (continued)

• DNS Service Attack
  – DNS Spoofing
    • Users or customers may be redirected to Web sites other than their intended destination
    • Should not be confused with phishing
    • May lead to customers giving their account information to hackers
  – DNS Overflows
    • May happen when there is a failure to check and verify the length of the host name
    • Could be used to gain superuser access to the system
Figure 11-5 DNS spoofing
Software Attacks (continued)

- Other software attacks include
  - Teardrop
  - Land
  - Charge
Isolated Attacks

• Comes from a single source
• It is easily countered by blocking traffic from that source
Distributed Attacks

- Come from multiple concurrent sources
- Much more difficult to block with ACLs or firewall rules
- Distributed denial-of-service, or DDoS, attack
  - Depends on the hacker’s ability to compromise information on a large number of systems
  - May require hundreds or thousands of compromised hosts to make a DDoS attack successful
  - Special tools used to attack a computer
Figure 11-6  DDoS basic attack
Distributed Attacks (continued)

• The process of DDoS is fully automated
• DDoS attack occurs in the following sequence:
  – Hacker identifies vulnerable hosts (100 or more)
  – Hacker gets access to these hosts after they are compromised
  – Hacker installs the tool needed to attack each host
  – Hacker uses the compromised hosts for future attacks
Known DoS Attacks

• Some known flood attacks are TCP SYN, SMURF, and Fraggle
• Denial of Service Database
  – At http://attrition.org/security/denial/
  – Has over 360 known DoS (and Ddos) exploits used on different targets
TCP SYN

• TCP SYN attack
  – Client and server exchange a sequence of messages after establishing a TCP connection
  – Uses the familiar three-way handshake of TCP

• Attacker establishes many half-connection
  – Data structure in memory that holds all the pending half-connections increases in size

• Hacker only has to use the IP spoofing technique to send excess SYN requests to the server
Figure 11-7  TCP SYN attack
SMURF

- ICMP is used to handle errors and exchange control messages on a network
- ICMP process is executed using the *ping command*

*Figure 11-8  ICMP echo*
SMURF (continued)

- Main components involved in a SMURF attack
  - Hacker, packet amplifiers or intermediate devices, and the target computer
- Recently, automated tools have been developed
  - That enable hackers to send these attacks simultaneously to several intermediaries
Figure 11-9  SMURF attack
Fraggle

- Fraggle attacks are like SMURF DoS attacks
  - But use UDP packets
- Attacker uses a spoofed IP address to broadcast hundreds of UDP packets across a network
- Intermediate devices reply to the victim computer by sending hundreds of UDP echo reply packets
- Best possible result is a system crash
  - At the very least, the attack will produce excess network traffic
Known DDoS Attacks

• DDoS tools use distributed technology to generate a large network of hosts
  – Hosts can attack thousands of computers via packet flooding
• Tools that can be used for DDoS attacks are Trinoo, Tribe flood network (TFN), and Botnets
Trinoo

- Distributed tool used to initialize coordinated UDP flood DoS attacks from multiple sources
- Trinoo network consists of a minute quantity of servers and a large number of clients
- Hacker computer is connected to a Trinoo master computer in a DoS attack utilizing a Trinoo network
- Hacker computer instructs the master computer to begin DoS attacks
  - Against one or more IP addresses
TFN

- Used to launch coordinated DoS flood attacks from multiple sources
- TFN has the capability to create packets with spoofed source IP addresses
- TFN network can generate DoS attacks such as:
  - UDP flood attacks
  - TCP SYN flood
  - ICMP echo request flood
  - ICMP directed broadcast
- TFN follows the same principle as Trinoo
Botnets

• **Botnets**
  – A variety of software DDoS
• A bot is a program that surreptitiously installs itself on a computer so it can be controlled by a hacker
• A botnet is a network of robot, or zombie, computers
  – Can harness their collective power to do damage
    • Or send out huge amounts of junk e-mail
Prevention and Mitigation of DoS and DDoS Attacks

• Network administrators can use packet filtering on the IP routers to give basic access control
• This often slows router performance to an unacceptable point
Prevention Methods

• **Network Address Translation (NAT)**
  – Prevents DoS by
    • Refusing network traffic from specific TCP ports
    • Limiting the network traffic coming from specific network addresses
    • Scanning the network traffic for viruses or undesirable applications
  • Solutions were designed to prevent DoS attacks on LANs and subnet systems
    – Not meant for a Web environment
Prevention Methods (continued)

- Cisco CSS 11000 series switches give comprehensive Web site and server-system security
- Switches provide site-level safety as follows:
  - DoS attack prevention
  - Firewall security
  - NAT
  - Load-balancing
Prevention Methods (continued)

- Other preventive measures
  - Implement router filters or ingress filtering
  - Computers should constantly be updated with the relevant security patches
  - Use intrusion-detection systems on networks containing Web servers
  - Disable any unnecessary services on your system
  - If supported, enable quotas on the operating systems

- Important to establish baselines for activities
Prevention Methods (continued)

• Measures for preventing DDoS attacks:
  – Filter all the RFC1918 address space by using access control lists (ACLs)
  – Apply ingress and egress filtering using ACLs
  – Rate-limit ICMP packets, if they are configurable
  – Configure the rate limiting for SYN packets
Mitigation of DoS and DDoS Attacks

• Use a tool such as Tripwire
  – To detect changes in the configuration information or on other files

• Problem with mitigation of DoS attacks
  – Attacks are easily mistaken for a small spike in network activity

• Upon detecting an attack
  – Initiate blocking packets from the origin IP or to the victim
Mitigation of DoS and DDoS Attacks (continued)

- Patch machines and applications
- Stay current on new reports of DoS and DDoS attacks and systems
- Run an IDS system that alerts you when the network is experiencing unusual traffic or activity