Network security (continued)

- Network perimeter defenses
  - Firewalls
  - Network intrusion detection/prevention
- Denial of service attacks

Firewalls – overview

- Firewalls restrict communication between an organization’s computers and the outside world
  - Keep the bad guys on the outside from exploiting vulnerabilities on the inside
  - Without restricting legitimate traffic
- NAT boxes implement a popular firewall policy
  - Allow internal clients to connect to outside servers
  - Do not allow inbound connections
- Two types of firewalls
  - Filter based (layer 4)
  - Proxy based (application layer)
Defense in depth

- Separate large network into smaller networks
  - Different parts of the organization have different protection needs / exposure / tolerance to lost functionality
    - E.g. laptops bring in trojans/viruses they catch while on the road
  - Different departments run different software packages with different vulnerabilities
  - Users in different departments need access to different servers / data sources
- Use multiple layers of firewalls (and other defenses)
  - Attacker must bypass multiple defenses

Firewalls

- Filtered Solution
  - Apply a set of rules to packets (based on headers)
  - Example of rules
    | action | source | dest | source port | dest port | comment |
    |--------|--------|------|-------------|-----------|---------|
    | allow  | OURG W | BLASTER | 25          | 2         | We don’t want this account.
    |        |        |        |             |           |         |
- Default: forward or not forward?
- Filtering on TCP flags can block connection from outside
- How dynamic?
- Access control rules (ACLs) also available in highest speed routers (but used differently)
Proxy-Based Firewalls

- Problem: complex policy
- Example: web server
- Solution: proxy
- Design: transparent vs. classical
- Limitations: attacks from within

Intrusion detection/prevention systems

- Main role: inspect packet payloads to detect attacks (e.g. buffer overflow) based on attack signatures
  - When match found, IDS logs alert, IPS drops packet
  - Thousands of signatures catch thousands of attacks against hundreds of applications for dozens of protocols
    - Needs defragmentation, stream reassembly, some L7 parsing
  - Legitimate traffic largely unaffected
  - IPS transparent to protocol endpoints
- Other roles: detect/block scans and various anomalies

Many IPSes out there

- Snort – most widely used, open source, developed by Sourcefire (makes money by selling GUI & services)
- Cisco IPS (formerly NetRanger)
  - IPS/IDS functionality present in many Cisco devices
- TippingPoint (now 3Com)

Signature with simplified Snort syntax describing fictitious vulnerability
Network security (continued)

- Network perimeter defenses
  - Firewalls
  - Network intrusion detection/prevention
- Denial of service attacks

Denial of Service (DoS) Attacks

- A general form of attacking inter-networked systems
  - Based on overloading end systems (or network)
  - Result is severe reduction in performance or complete shutdown of target systems
- Focus of attack can be links, routers (CPU) or end hosts
- Flooding attacks pretty common nowadays
- Other most general form of attack is a break in
  - Port scans
  - Buffer overflows
  - Password cracking…

Overloading a System

- The goal of DoS is to drown legitimate traffic in a sea of garbage traffic
  - Clients experience delays due to congestion
    - Dropped packets lead to exponential backoff in timeouts
  - Routers can become overloaded
- Servers become overloaded by increased number of connect requests
  - TCP connection setup requires state on server
  - Server is required to respond to SYN from clients
  - Clients don’t respond to server’s response
IP Spoofing
- Insert a different source IP address in TCP and IP headers
  - DoS attackers spoof for two reasons
    - They don’t want to be discovered
    - Spoofing can add additional load
- If attacker spoofs a legitimate IP address
  - Reset can be triggered by either attacked host or actual IP host
    - Frees resources immediately on server
    - Carefully chosen sequence #s block new connections from host
- Attackers spoof with random IP addresses
  - Server response to client SYN will be lost
  - Server will not free resources for 75 seconds (typically)
  - SYN cookies on allow server kernel not to keep state

Key Elements of DoS Attack
- Expansion in required work
  - Easy for me, harder for you
  - Expansion in IP spoofing
    - Me: generate SYNs as fast as possible (microseconds)
    - You: Timeout a SYN open every 75 seconds
- Best effort protocols
  - Drop tail queues
  - No source specificity
  - Clients can be starved or slowed to crawl

DoS Attack Characteristics
- Expansion makes a only a few systems necessary
  - DDoS: attack from as many places as possible
    - Enables better utilization of network resources
    - Helps to prevent countermeasures
    - Helps to obscure attackers
- DoS software readily available
  - Most found in IRC chat rooms
- DoS attacks frequently preceded by break-ins to install DoS software onto “zombies”
  - Enables even more anonymity for attacker
Things making DoS Attacks easy

• Lots of systems
• Large networks
• Naïve users with high speed Internet access
• Savvy bad guys
• Lots of free DoS software
• Poor operating and management policies
• Hugely complex software (on endhosts) with lots of well publicized holes
• Lack of means for stopping attacks

Dealing with DoS Attacks

• Don’t reserve state until receipt of client ACK
  – DOS attackers using spoofing don’t send these
    • Otherwise they would have to keep state
  – Use of crypto to avoid saving state
    • Send one-use key with server response to SYN
    • Response ACK must return key
• IP traceback methods were popular research topic
• Use intrusion detection/prevention tools
  – Traffic to victim redirected through “traffic scrubbing” centers
  – There are lots of companies in this space!

Example of (D)DoS

• Code Red Worm
  – Released and identified on July 19, 2001
    • Infected over 250k systems in 9 hours
  – Takes advantage of hole in IIS on Win NT or Win 2k
    • And the fact that most people don’t know IIS ON is default
  – Infected systems are completely compromised
  – Code Red installs itself in OS kernel
    • Small and efficient
    • V1 could be eliminated by reboot
  – Spends half its time trying to infect other systems, and half its time DoS’ing the White House and Pentagon