CSE331: Introduction to Networks and Security

Lecture 35
Fall 2002
Announcements

• Homework 3 Due Friday

• Project 4 Deadline Extended
  – Due: Monday, December 9th

• December 9th Review Session

• Final Exam Location
  – Moore 212
  – Tues. 17 Dec.
  – 8:30 – 10:30 AM
TEMPEST Security

• Transient Electromagnetic Pulse Emanation Standard
  – (Or?) Temporary Emanation and Spurious Transmission
  – Emission security (Van Eck phreaking)
  – computer monitors and other devices give off electromagnetic radiation
  – With the right antenna and receiver, these emanations can be intercepted from a remote location, and then be redisplayed (in the case of a monitor screen) or recorded and replayed (such as with a printer or keyboard).
TEMPEST

• Policy is set in National Communications Security Committee Directive 4

• Guidelines for preventing EM reception
  – Shield the device (expensive)
  – Shield a location (inconvenient?)

• Not a risk?
  – Most of the guidelines are classified!
Denial of Service

• 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
  
  – attempts to disrupt connections between two machines, 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

http://www.cert.org/tech_tips/denial_of_service.html
Impact

• Denial-of-service attacks can essentially disable your computer or your network.
  – this can effectively disable your organization.

• Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site.
  – This type of attack is sometimes called an *asymmetric attack*.
  – An attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.
Modes of Attack

• Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:
  – consumption of scarce, limited, or non-renewable resources
  – destruction or alteration of configuration information
  – physical destruction or alteration of network components
Consumption of Scarce Resources

- Resources:
  - network bandwidth
  - memory and disk space
  - CPU time
  - data structures
  - access to other computers and networks
  - certain environmental resources such as power, cool air, or even water.
Network Connectivity

- Denial-of-service attacks are most frequently executed against network connectivity.
- The goal is to prevent hosts or networks from communicating on the network.
- An example of this type of attack is the "SYN flood" attack.
TCP: Three-Way Handshake

Active participant (client)  Passive participant (server)

SYN, SequenceNum = \(x\)

SYN + ACK, SequenceNum = \(y\),

Acknowledgment = \(x + 1\)

ACK, Acknowledgment = \(y + 1\)
Partially Open TCP Sessions

• A *half-open connection*  
  – After the server system has sent an acknowledgment (SYN-ACK)  
  – But before it has received the ACK  

• The server has built a data structure describing all pending connections.  

• The server can only store a fixed number of half-open connections  
  – When the table is full, new requests are dropped  
  – There is a time out, but flooding exhausts resources
IP Spoofing

• The attacking system sends forged SYN messages to the victim server system
• These appear to be legitimate but actually reference a client unable to respond to the SYN-ACK.
• The source addresses in the SYN packets are forged.
  – No way to determine its true source.
Asymmetry

• SYN flood attacks do not depend on the attacker being able to consume your network bandwidth.
  – The intruder is consuming kernel data structures involved in establishing a network connection.
  – Can execute this attack from a dial-up connection against a machine on a very fast network.

• This is a good example of an asymmetric attack.
Filtering

• With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets.

LAN → Firewall → INTERNET

Make sure outgoing packets have SRC in LAN

Make sure incoming packets have SRC not in LAN
UDP “Packet Storm”

- chargen service
  - Generates a continuous stream of character output in UDP packets
  - Used for testing network bandwidth

- echo service
  - Accepts a UDP packet (i.e. telnet keystroke) and repeats it back to the sender

- Connect the chargen service to the echo service!
  - Uses up all network bandwidth between the services
Consumption of Other Resources

- Generate many processes
  - As in the Internet Worm

- Consume disk space
  - E-mail bomb/spam flood
  - Intentionally generate errors that must be logged
  - Put large files in anonymous FTP directories

- Prevent login
  - Some sites “lockout” accounts after a certain number of failed login attempts
  - Write a script to lockout everyone
  - Works against root
Destroying or Altering Config. Info.

• If an intruder can change routing tables, things are bad
  – Completely disable the network

• If an intruder can modify Windows registry information things are bad
  – Can disable certain OS functions
Physical Destruction of Network

• Physical security
• Guard against unauthorized access to:
  – Computers
  – Routers
  – Network wiring closets
  – Network backbone segments
  – Power and cooling stations
  – Any other critical components of your network.
Prevention & Response 1

• Implement router filters
  – Lessen exposure to certain denial-of-service attacks.
  – Aid in preventing internal users from effectively launching denial-of-service attacks.

• Disable any unused or unneeded network services
  – Limits the ability of an intruder to take advantage of those services to execute a denial-of-service attack.
Prevention & Response 2

• Enable quota systems on the operating system
  – Disk quotas for all accounts
  – Partition file system to separate critical functions from other data

• Observe the system performance
  – Establish baselines for ordinary activity.
  – Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.
Prevention & Response 3

- Invest in and maintain "hot spares"—Machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules—particularly for important configuration information.