SE 4C03 Winter 2002

06. Computer and Network Security Threats

Instructor: W. M. Farmer

Revised: 28 February 2002

Kinds of Threats

- Physical threats to hardware
- Faulty software
- Malicious software
- Unauthorized access
- Denial of service attacks
- Network probing
- Network manipulation
- Resource theft

Physical Threats to Hardware

- Hardware theft
- Hardware damage
- Unauthorized physical access to hardware

Faulty Software

- Malfunctioning software
  - Poorly designed (does not meet requirements)
  - Poorly implemented (does not meet specification)
- Software with exploitable bugs
  - Operating system releases
  - Software allowing buffer overflow
- Software with exploitable weaknesses
  - Flawed communication protocols
  - Network services
- Misconfigured software
  - Operating system security mechanisms
  - Web servers

Malicious Software

- A **virus** makes copies of itself and may be malicious in various ways
- A **worm** spreads across networks and may be malicious in various ways
- A **Trojan horse** has a hidden, illicit function
- A **logic bomb** has a hidden behavior that goes off when certain conditions are satisfied
- A **hacker's toolkit** is a collection of programs that enable one to probe and attack computers and networks

Unauthorized Access

- Surmount authentication
  - Password guessing
  - Password interception
  - Password cracking
  - Session replaying
- Session hijacking
- Identity spoofing
  - Source address spoofing
  - Domain name spoofing
- Misconfigured access control
  - SUID (Set User ID on execution) programs and scripts
  - SGID (Set Group ID on execution) programs and scripts

Denial of Service Attacks

- Overload a host or network
  - SYN flood: send to a host a flood of packets that request the creation of TCP connections
  - Broadcast storm
  - E-mail attacks
  - Virus and worm attacks
  - Process overload attacks
- Disable a host or network
  - Disk partition attacks (/, `/var`, `/tmp`, swap)
  - ICMP-based attacks

Network Probing

- Network probing tools
  - Ping
  - Traceroute
- Port scanning
  - TCP SYN scanning
  - TCP SYN half scanning
  - TCP FIN scanning
- Network analysis tools such as SATAN
- DNS

Network Manipulation

- Routing modification
  - Routing protocols without authentication such as the Routing Information Protocol (RIP)
  - ARP
- DNS modification
- Source routing
- Packet sniffing

Resource Theft

- CPU cycles
- Disk space
- Hosts
- Communication resources