Hostile Code

Several Examples

• Melissa Virus
  – Spread as Email attachment
• I Love You worm
• Smurf
  – A Denial of Service attack involving forged ICMP packets sent to a broadcast address

Example of Attacks

• Program Level Security
  – Non-malicious Program Errors: Buffer Overflow, Format String...
  – Malicious Codes: Trojan Horse, Logic Bomb, Virus, Worm...
• Network Attacks
  – Threat Precursors: Port Scan, Social Engineering, Reconnaissance, OS and App. Fingerprinting
  – Protocol Flaws: Impersonation
  – Spoofing: Session Hijacking, Man-in-the-Middle
  – Message Confidentiality Threat
  – Message Integrity Threats
  – Denial of Service: Connection Flooding (Ping of Death, Smurf), Syn Flood, DNS attack
  – Distributed Denial of Service

Several Examples

• IRC Bots
• NetBus
• Back Orifice
  – A backdoor program
  – Designed for remote system administration
  – http://www.bo2k.com
• Internet Bots
• Bombs:
  – Logical Bombs
  – Time Bombs

Vulnerability Scanner

• Nessus
  – http://www.nessus.org/