Malicious Code
Vulnerability Analysis
Intrusion Detection

Lecture 11

Nov 22, 2005

What is Malicious Code?

- Set of instructions that causes a security policy to be violated
  - Is an unintentional mistake that violates policy malicious code? (Tricked into doing that?)
  - What about “unwanted” code that doesn’t cause a security breach?
- Generally relies on “legal” operations
  - Authorized user *could* perform operations without violating policy
  - Malicious code “mimics” authorized user

Types of Malicious Code

- Trojan Horse
  - Trick user into executing malicious code
- Virus
  - Replicates and inserts itself into fixed set of files
- Worm
  - Copies itself from computer to computer