Virus & Worm

Viruses: The Principle

- Virus attaches itself to a host that can execute instructions contained in the virus.
- When the host is invoked, the virus copies itself to other locations on the system.

Trojan Horses

- Seemingly useful program that contains code that does harmful things
  - Perform both overt and covert actions
- Frequently embedded in applets or games, email attachments
- Trojan horse logins, spoof authentication or webpage forms

Key Loggers and Spyware

- Gather information from computer
  - Send back to the central office
- From key loggers can gather
  - Passwords
  - Confidential communication
  - Keep track of your kids/employees
- From spyware can gather
  - Web browsing habits
  - Gather marketing information

Rootkits

- Insert file filters to cause files or directories disappear from normal listings
  - Can replace Windows API pointers (user mode)
  - Can also replace syscall table pointers
- Both require privilege, but most Windows installs require privilege anyway
  - The power of extensibility used for the dark side
- Techniques apply equally well to Linux and Mac

Virus Operation

- Virus Phases:
  - Dormant: Waiting on trigger event
  - Propagation: Replicating to programs/disks
  - Triggering: By event to execute payload
  - Execution: Executing payload
- Details usually Machine/OS specific
  - Exploits different features or weaknesses