Malware – malicious software (may or may not be destructive, depending on intent)
  
  - 2 categories of classification
    - How it propagates/spreads
    - What its payload does/what it is intended to do
  
  - Ways of delivery include
    - Could already exist in a file system
    - By visiting websites (called a drive-by) or though downloads
    - Social engineering attacks
  
  - Attack kit – A way to create new malware; comes with supplied propagation/payload methods

Viruses – tricks system into replicating it, like a biological virus
  
  - If attached to an executable, the virus can do anything the program can
  
  - 4 phases
    - Dormant phase – it is idle
    - Triggering phase – wakes up
    - Propagation phase – spreads around the disk
    - Execution phase – after it has spread, execute/do what it was supposed to do
  
  - Viruses hide themselves by:
    - Metamorphic virus - changing meta data
    - Encrypted virus - hey can be encrypted
    - Use scripting to keep it remote rather than local
    - Polymorphic virus - changes after every infection
    - Stealth virus - can hide in plain sight

Worms – actively looks for things to attack, doesn't wait to execute like a virus
  
  - Can use network connections to spread from system to system
  
  - Replication methods:
    - Emails a copy of itself to other systems
    - Creates a copy of itself on removable media
    - Executes a copy of itself on another system
    - Remotely copies itself to another system
  
  - Scanning/Fingerprinting – when the worm searches for other systems to infect.
  
  - Morris Worm – one of the first famous worm infections
    - Designed for UNIX systems