**Module 5 Malware**

**5.1 Malware Worms Trojans**

**Worms**

1. Self-replicating & self-propagating program that uses networking mechanisms to spread itself
2. Eats up resources
3. Examples
   1. Code Red – exploited ISS servers in 2001 suing buffer overflow
   2. SQL Slammer – DoS worm that attacked buffer overflow weaknesses in Microsoft SQL services
      1. Also used UDP & was small in size
   3. Nimda – spread through open network shares, websites & email
      1. Also used backdoors that were left on machines by Code Red

**Trojans**

1. Appear to perform desired function but actually performs actions w/o user’s knowledge intended to steal info/harm user’s system/data
2. Covert channel – used to transmit info in way that is illegal/impossible
   1. Violates security policy on system
3. Overt channel – used to send info/perform other actions in legit way (Eg. TCP/IP)
4. Indications of trojan infection
   1. CD drawer randomly opens/closes
   2. Comp screen inverts/flips
   3. Documents randomly print
   4. Browser redirection
   5. Mouse pointer disappears
5. Associated ports
   1. Back Orifice – UDP 31337/31338
   2. Beast – TCP 6666
   3. Whack-a-Mole – TCP 12361/12362
   4. Girlfriend – TCP 21544
   5. Netbus 2 pro – TCP 20034
   6. Timbuktu – TCP/UDP 407