I. Worms and Viruses

1. Worms
   - They are self-spreading
   - They enter mostly thru some security flaws
   - The 1st worm is the Morris Worm created in 1987.

2. Viruses
   - They need some human interactions
   - Human interactions refer to downloading a file, or opening email attachments.

II. Relationships between Biological diseases and Computers Viruses/Worms

1. Common points
   - Spread: They both self-spread. They require some contact
   - They have been around for a while

2. Differences
   - Speed: Computers are faster
   - Range: Biological diseases are localized whereas computers virus are global ie could access farther clients thru the internet or other means.
   - Existence: Biological diseases are independent whereas computers act typically at behest of the creator

III. Is there a “universal worm/virus catcher”?  
The answer is NO. The following is a proof:

Let’s assume that C is catcher program, and P is any program so that  
C(P) = 0, if P is not a worm  
C(P) = 1, if P is a worm

Saying that there is no universal worm catcher is equivalent to claiming that this theorem is true: “There does not exist C such that C(P) = 1, if and only if P is a worm”

Proof by Contradiction:
→ Let’s assume that such a C exists
→ Let’s consider P to be a program with the following pseudocode:
   *Run C on P
   *if C(P) = 0, then replicate and infect someone (a)
   *if C(P) = 1, then exit (b)
→ Suppose now that \( C(P) = 0 \). Then it is the wrong answer because \( P \) in fact is acting like a worm due to the definition of (a)
→ Suppose also that \( C(P) = 1 \). Then it is also the wrong answer because \( P \) is entirely harmless due to the definition of (b)

In either situation, there is a contradiction since the last 2 suppositions are wrong. Hence, the assumption that a catcher program \( C \) exists is False. Therefore, the theorem is true.

IV. DoS Attacks.

1. Honey Pots & Honey Nets
   - Sting Operation
   - Virtual environment where one can monitor the attacker (human, worm/virus).

2. Script kiddies
   - Young inexperience hackers
   - Running other people’s scripts
   - They often get caught

3. Telescopes & Backscatters
   Telescopes are mostly large blocks of IP addresses on which little or no legitimate traffic exists. Telescopes yield a view of certain remote network events and could detect the presence of DoS attacks, infection of hosts by Internet Worms.

When a DoS Attack is detected and ISPs are contacted to troubleshoot the issues, they would usually first put the IP address offline. This causes the Border Routers to reply to the spoofed sources saying ICMP Host not reachable. The ISP will listen in on a telescope and look at the source address of these ICMP packets to find which Border Router the attack packets are transiting. Once the Border Router is found a filter will be set by the ISP to eliminate the attack packets and the IP address will be brought online again.
4. Types of DoS attacks

- **Local**: They eat up local resources on a machine. E.g.:
  - Intensive database applications
  - Screen resources
  - Delete drivers
  - Fork bombs

- **Distributed**:  
  - **Smurf Attack**: In this case, the attacker sends multiple ICMP echo requests to a large number of computers. The source IP address is spoofed as the victim’s IP addresses. Hence, all the echo replies are sent back to the victim.

In this smurf attack case, the attacker will experience low bandwidth, but this could be avoided if other machines are hijacked by the attacker.

Target Networks with broadcast addresses left open are often attacked. During open broadcast attacks, all computers in the gateway’s subnet will be affected.

- **SYN Flood Attack**: In this case, the attacker sends a large number of SYN packets to the victim. By trying to respond to each of the SYNs, the victim will quickly fill up its queue of allowed connections, making the computer unable to reach the internet.

To maintain this flood, the attacker will continue to send SYN packets at the same interval it takes the queue to empty.
Ways to mitigate the SYN attack:

- Decrease the timeout
- Throttle or filter the number of concurrent connections per source IP.
- Increase the size of queue

- Use Syn-cookies, which allow intended victims to bypass the system of keeping track of connections. Syn-cookies use a hash function that combines the 4-tuple (source IP, destination IP, source port #, destination port #) with the time of transaction and personal information. From this hash function, a special number (sequence number) is assigned to each host requesting a conversation thru a SYN-ACK. That sequence number will be needed by the sender to establish a connection after a SYN-ACK-ACK, otherwise, the connection will be dropped.
V. Why is spoofing allowed? Why not source filtering?

- Mainly because of multi-home ISPs: households may have multiple ISPs, therefore multiple IP addresses and it would be hard for ISPs to keep track of the other IPs owned by each household.
- The internet does not currently concern itself with the validity of source IP addresses in packets.