Week 13 Questions

Lecture 71

1. In the consumer problem, the attacker blocks the client from communicating with the server. In the producer problem, the attacker overwhelms the server with requests. The producer problem is more prevalent.
2. An attacker forges the return address on the SYN packets and floods the server with these. This leads the server to fill its table with only half-open connections.
3. They could take up a lot of resources, disallow connections by slower clients, and matching return addresses are hard to determine.

Lecture 72

1. Not very well. It is hard to determine if a packet is legitimate or fake.
2. Intrusion detection tries to determine if an attack on the system has occurred. Intrusion prevention tries to prevent an attack on the system.
3. By over-provisioning the network, there would be too many servers to be overwhelmed. Filtering attack packets to distinguish between attack packets and regular packets. Slowing down processing would disadvantage attackers who may be sending a lot of bad packets. "Speak-up" solution is when an attack occurs, request additional traffic from all requestors. Attackers usually are maxed out so the legitimate packets will be more than the bad packets.

Lecture 73

1. False negatives are attacks that go undetected whereas false positives are mis-behaviors classified as attacks. False positives are worse because information never gets there.
2. Accurate detects all genuine attacks therefore there are no false negatives. Precise never reports legitimate behavior as an attack therefore there are no false positives.
3. It is hard to do both simultaneously. You can block everything so no attacks happen or you can report nothing so legitimate behavior is not reported.
4. An effect is attributed to an incorrect cause. In IDS, false positives can occur and with high probability.

Lecture 74

1. If date is between 1st and 19th of the month, generate a random list of IP addresses and attempt to infect those machines. It attempted to launch a DoS flooding attack on *www1.whitehouse.gov*.
2. Identical lists of IP addresses used on each infected machine. Each infected machine probed the same list of machines, so the worm spread slowly.
3. The worm was stored in memory which would be flushed with a simple reboot.
4. A random seed was used to create random IP addresses. More random list of IP addresses created leading to more computers infected.

Lecture 75

1. It exploited the same vulnerability as Code Red.
2. Machines on the same network or subnet are likely to be running similar software. The elaborate propagation allows for infection of machines on the same network with similar machines.
3. Installs a mechanism for remote, root-level access to the infected machine. This backdoor allows any code to be executed, so the machines could be used as zombies for future attacks.
4. There are a large number of vulnerable computers. This worm could be used again.
5. You should install patches when they are released.