CS 4910 Introduction to Computer Security
Assignment 3

1. Explain what a Denial-of-Service attack is and list three examples.
Solution: A Denial-of-Service (DoS) attack is an attempt to make a system or network unavailable by overwhelming it with excessive traffic or requests, preventing legitimate users from accessing the service. Common examples of DoS attacks include:

- SYN flood: The attacker sends a large number of TCP SYN requests but never completes the handshake, exhausting the server's connection resources.
- ICMP (ping) flood: The attacker overwhelms a target with a high volume of ICMP echo requests, consuming bandwidth and processing capacity.
- DNS amplification attack (a form of distributed DoS): The attacker sends small spoofed requests to DNS servers, which generate large responses that are redirected to the victim, amplifying traffic volume.

2. Explain why a SYN flood attack can work and how to mitigate it.
Solution: A SYN flood works because of how the TCP three-way handshake allocates resources. It exploits the TCP handshake by sending many SYN requests with spoofed source IP addresses. The server replies with SYN-ACK to these (often nonexistent or unreachable) addresses and allocates resources for half-open connections. Because the final ACK never arrives, the backlog queue fills up, preventing the server from accepting legitimate connections.
The *mitigation* can be: 1) SYN cookies: Avoid allocating state until the final ACK is received; encode state in the SYN-ACK, 2) Reduce SYN timeout / increase retries control: Frees half-open entries faster, and 3) Rate limiting / filtering: Limit incoming SYN rate or block suspicious sources (e.g., via firewalls).

3. In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). 1) How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? 2) How many of these packets per second must the attacker send to flood a target organization using a 2-Mbps link? 3) How many of these packets per second must the attacker send to flood a target organization using a 10-Mbps link? (Hint: 1 byte = 8 bits. 1-Mbps = 1000000 bits)
Solution: In a DoS attack using ICMP Echo Request (ping) packets 500 bytes in size, to flood a target organization using a 0.5 Megabit per second (Mbps) link the attacker needs 500000 / (500 x 8) = 125 packets per second.
On a 2-Mbps link its 2000000 / (500 x 8) = 500 packets per second.
On a 10-Mbps link its 10000000 / (500 x 8) = 2500 packets per second.

4. What is the ARP spoofing attack? Explain this attack using an example.

Solution: An attacker sends fake ARP messages onto a local network, linking an attacker's MAC address with the IP address of a legitimate computer or server on the network.

5. Give an example to explain the DNS hijacking attack. Why can a DNS cache be easily poisoned, and how can it be prevented?
Solution: The attacker redirects traffic from legitimate servers to fraudulent ones by altering DNS server settings or DNS records.

6. We have the following ruleset for the firewall. 1) Explain the ruleset. 2) Can the ruleset filtering address spoofing? Why?

```
allow TCP *:* -> 22.33.44.55:80
allow TCP (our-hosts):* -> *:*
allow TCP *:* -> (our-hosts):* (if ACK bit set)
drop * *:* -> *:*
```

Solution:
1) We allow inbound connections to server 22.33.44.55 on port 80. The allowed inbound packets are associated with an outbound connection, while the disallowed inbound packets are associated with an inbound connection. We allow all outbound connections. Other connections will be dropped.
2) No. The attacker can spoof the source IP address as an insider host and perform TCP handshakes to establish a TCP session.

7. What are the differences between firewalls and intrusion detection systems?
Solution: Firewalls control what gets in or out based on rules, and IDS systems monitor and alert on suspicious activities.

8. What are the two intrusion detection approaches? Explain the advantages and disadvantages of each approach.
Solution: The two methods are signature-based detection and anomaly detection.
The *advantages* of signature-based detection are (1) simple; (2) can detect known attacks; (3) knows which attack at the time of detection; and (4) efficient.
The *disadvantages* of it are (1) signature files must be kept up to date; (2) the number of signatures may become large; (3) it can only detect known attacks; 4) variations on known attacks may not be detected.
The *advantages* of anomaly detection are (1) it can detect unknown attacks, and (2) it can be more efficient.
The *disadvantages* of it are (1) the reliability is unclear because of high false positives and false negatives; (2) the detection indicates something unusual, but lacks specific information on a possible attack.