Week 8 Revision Notes

Week 8 - Network Security: Protocol Vulnerabilities and Threats

1. Key Security Terms

- **Vulnerability**:
  - A vulnerability is a weakness in a system or network that attackers can exploit to cause harm.
  - Example: An outdated software version without security patches is vulnerable to attacks.
- **Threat**:
  - A potential cause of harm to a system, organization, or data, such as hackers or natural disasters.
  - Example: A threat could be an attacker trying to gain unauthorized access to a system.
- **Cyber Risk**:
  - The potential that a threat could exploit a vulnerability, resulting in loss or damage to data, systems, or reputation.

2. Internet Protocol (IP) Vulnerabilities

- **IP Protocol Basics**:
  - The **Internet Protocol (IP)** is responsible for routing packets across networks.
  - **Key Fields in the IP Header**:
    - **Version**: Indicates IPv4 or IPv6.
    - **TTL (Time to Live)**: Limits the lifespan of a packet to prevent infinite loops.
    - **Checksum**: Detects errors in the header.
- **IP Vulnerabilities**:
  - **IP Spoofing**:
    - Attackers send packets with a fake source IP address, disguising their identity.
  - **Denial of Service (DoS)**:
    - Attackers flood a network with traffic, overwhelming systems and causing downtime.

3. Address Resolution Protocol (ARP)

- **Purpose of ARP**:

    - Resolves IP addresses to MAC addresses within a Local Area Network (LAN).
    - **ARP Process**:
        - **Direct Delivery**: If sender and receiver are on the same network, the sender requests the MAC address of the receiver.
        - **Indirect Delivery**: If sender and receiver are on different networks, the sender first gets the MAC address of the gateway (router) to forward packets.
- **ARP Vulnerabilities**:
    - **ARP Poisoning (ARP Spoofing)**:
        - Attackers send fake ARP messages, associating their MAC address with the IP of another device, often to intercept traffic (Man-in-the-Middle attack).

4. Internet Control Message Protocol (ICMP)

- **ICMP Role**:
    - ICMP is a supporting protocol used for error messages and diagnostics (e.g., **ping** and **traceroute**).
    - **Common ICMP Messages**:
        - **Echo Request/Reply**: Used by `ping` to check if a device is reachable.
        - **Destination Unreachable**: Indicates that a destination cannot be reached.
        - **Time Exceeded**: Sent when a packet's TTL (Time to Live) expires.
- **ICMP Vulnerabilities**:
    - **ICMP Redirect Attack**:
        - Attackers use ICMP messages to reroute packets to a different location.
    - **Ping of Death**:
        - An attacker sends an oversized packet to cause a buffer overflow, potentially crashing the target system.

5. Transmission Control Protocol (TCP)

- **TCP Features**:
    - **Reliable and Connection-Oriented**: Ensures data reaches its destination in the correct order.
    - **Three-Way Handshake**:
        1. **SYN**: The client sends a synchronization request.
        2. **SYN-ACK**: The server acknowledges and syncs back.
        3. **ACK**: The client confirms, and the connection is established.
    - **Four-Way Termination**:

        - Used to close a TCP connection, involving a sequence of `FIN` (finish) and `ACK` messages.
- **TCP Vulnerabilities**:
    - **SYN Flooding**:
        - Attackers initiate many connections without completing them, overloading the server and causing denial of service.
    - **Sequence Prediction**:
        - Attackers predict sequence numbers to hijack a TCP session, inserting malicious data.

6. Dynamic Host Configuration Protocol (DHCP)

- **DHCP Role**:
    - DHCP assigns IP addresses to devices automatically, simplifying network management.
    - **DHCP Lease Process**:
        1. **DHCPDISCOVER**: The client requests an IP address.
        2. **DHCPOFFER**: The server offers an IP address.
        3. **DHCPREQUEST**: The client accepts the offer.
        4. **DHCPACK**: The server confirms and finalizes the lease.
- **DHCP Vulnerabilities**:
    - **DHCP Spoofing**:
        - Attackers set up a fake DHCP server to assign malicious network settings, such as a false default gateway.
    - **DHCP Starvation Attack**:
        - Attackers flood the server with requests until it runs out of IP addresses, preventing legitimate clients from connecting.

7. Domain Name System (DNS)

- **DNS Purpose**:
    - Translates human-readable domain names (e.g., `example.com`) into IP addresses.
- **DNS Vulnerabilities**:
    - **DNS Cache Poisoning**:
        - Attackers insert false DNS entries, redirecting users to malicious sites.
    - **DNS Flood Attack**:
        - Overwhelms DNS servers with excessive requests, causing denial of service.

Summary of Protocol Threats

Protocol	Vulnerabilities/Threats
IP	IP Spoofing, Fragmentation Attacks
ARP	ARP Cache Poisoning, Man-in-the-Middle (MITM) Attack
ICMP	Redirect Attack, Ping of Death
TCP	SYN Flood, Sequence Prediction
DHCP	DHCP Spoofing, Starvation Attack
DNS	Cache Poisoning, DNS Flood Attack

8. Types of Security Attacks

- **Active Attacks**:
  - Involve data modification or malicious insertion into a network. Examples include:
    - **Masquerade**: Attacker impersonates another user.
    - **Replay Attack**: Attacker intercepts and retransmits messages to gain unauthorized access.
    - **Modification of Messages**: Altering data in transit.
    - **Denial of Service (DoS/DDoS)**: Overwhelming a network or system to disrupt service.
- **Passive Attacks**:
  - Attacks that monitor or capture data without altering it, such as:
    - **Traffic Analysis**: Monitoring data flow to infer information.
    - **Eavesdropping**: Listening in on private communication.