Advanced Cybersecurity Concepts

1.Explain MAC spoofing and Email spoofing

ANS: MAC Spoofing: MAC (Media Access Control) spoofing is the act of changing a device's MAC address (its hardware/network interface identifier) to some other value.

Email Spoofing: Email spoofing is forging the "From" address of an email so that it appears to come from someone else.

2. Perform practical of MITM tool and social engineering Tool

ANS: MITM Tool Set up your lab:

- Use at least 3 VMs: Attacker (Kali), Victim, Target (e.g., web server).
- Put them on an internal network / host-only network so you don't affect real networks.

2. **Install MITMf** (Man-in-the-Middle Framework):
    - There are guides for installing MITMf on Kali.
    - Once installed, run it in MITM mode.
3. **Use MITMf to intercept / manipulate traffic**:
    - For example, perform ARP spoofing to position yourself between the victim and the gateway.
    - Capture HTTP traffic, inject JavaScript, sniff credentials, etc.

3. Explain Kali linux tool SYN Flooding Attack using Metasploit

ANS: SYN Flood Attack: A Denial-of-Service (DoS) attack where the attacker sends a large number of TCP SYN packets (to initiate TCP handshake), but never completes the handshake. The target system allocates resources for each half-open connection, eventually exhausting its capacity.

Using Metasploit on Kali:

- Metasploit has auxiliary modules that can be used for DoS / flooding attacks. For example, one can use its auxiliary/dos modules (depending on version) to launch a SYN flood.
- In practice:
    1. Open msfconsole.
    2. use auxiliary/dos/tcp/synflood.

3. Set options: target host RHOST, target port RPORT, maybe number of packets, source IP .
4. Run the module and monitor the effect on the target

4. Find online email encryption service

ANS: some well-known online email encryption services:

- **Proton Mail**
- **Tutanota**
- **Hushmail**
- **Mailvelope**
- **Mynigma**

5. Types of Firewall

ANS: The major types of firewalls:

1. **Packet-Filtering Firewall**
   - Examines packet headers (IP, port, protocol) to allow/block.
   - Works at OSI Layer 3 (Network).
   - Pros: simple, fast. Cons: no deep content inspection, vulnerable to spoofing.
2. **Stateful Inspection Firewall**
   - Tracks connection state (e.g., TCP handshake) and uses that context to filter.
   - More secure than packet filtering; can prevent certain attacks.
3. **Proxy Firewall (Application-level Gateway)**
   - Acts as an intermediary (proxy) for client-server connections.
   - Operates at Application Layer (OSI Layer 7).
   - Provides deep inspection, can filter based on application data/content.
4. **Next-Generation Firewall (NGFW)**
   - Combines stateful firewalling + deep packet inspection (DPI) + intrusion prevention + application-level awareness.
   - Can control traffic based on application, user identity, and content.

6. Explain Evading Firewalls

ANS: Evading a firewall means getting around or bypassing its filtering mechanisms. There are some common techniques and considerations:

- **Packet Manipulation / Fragmentation**: Split malicious payload over multiple small packets so that firewall signature rules can't detect them.
- **Protocol Tunneling / Encapsulation**: Use allowed protocols to tunnel disallowed traffic (e.g., SSH tunneling, HTTP tunneling).
- **Using Encryption / SSL**: Tunnel malicious traffic over SSL/TLS so firewall can't inspect the payload (if firewall does not perform deep SSL inspection).
- **Encoding**: Encode payload to avoid detection.
- **Using Non-standard Ports**: Use ports that are allowed by firewall but not heavily monitored, instead of default exploit ports.
- **HTTP Request Manipulation**: For web app firewalls (WAFs), attackers can use parsing discrepancies or malformed HTTP requests to bypass rules. For example, recent research shows bypassing WAFs by exploiting parsing ambiguities.
- **Active Reconnaissance / Firewalking**: Use techniques like firewalking to map which ports/protocols are allowed by the firewall.
- **Use of NAT / Proxy**: Use intermediate proxy machines to route traffic, so firewall sees only the proxy's traffic, not the original malicious source.