Cybersecurity Practical and Theory

## 1. Explain MAC spoofing and Email spoofing

MAC spoofing involves changing the MAC address of a device to impersonate another device. Email spoofing involves forging the sender's address on an email to make it appear as if it came from someone else.

## 2. Perform practical of MITM tool and social engineering Tool

Use tools like Ettercap or Wireshark for MITM attacks to intercept traffic. For social engineering, tools like SET (Social Engineering Toolkit) can simulate phishing and other manipulation techniques.

## 3. Explain Kali linux tool SYN Flooding Attack using Metasploit

In Kali Linux, use Metasploit's auxiliary modules like 'dos/tcp/synflood' to perform SYN Flood attacks by sending a large number of SYN packets to target to exhaust server resources.

## 4. Find online email encryption service

ProtonMail (https://protonmail.com) and Tutanota (https://tutanota.com) are popular online email encryption services offering end-to-end encryption.

## 5. Types of Firewall

Types include Packet Filtering Firewall, Stateful Inspection Firewall, Proxy Firewall, and Next-Generation Firewall (NGFW).

## 6. Explain Evading Firewalls

Firewall evasion techniques include IP fragmentation, tunneling traffic through allowed protocols (like HTTP or HTTPS), and using encrypted payloads or polymorphic code.

## 1. What is Session Hijacking Explain with Techniques?

Session hijacking is taking over a valid user session. Techniques include stealing session cookies, using XSS, or IP spoofing.

## 2. Find DoS/DDoS Attack Tools

Popular tools include LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon), HULK, and Slowloris.

## 3. Explain SYN Flooding Attack with example

SYN flooding is a DoS attack where attackers send multiple SYN requests without completing the handshake. Example: sending continuous SYN packets to a web server without responding to SYN-ACK.

## 4. List of Web App Hacking Methodology

Steps include Information Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting.

## 5. SQL Injection Methodology

SQL Injection involves inserting malicious SQL queries through input fields. Steps: Identify input points, inject payload, extract data or bypass login.

## 6. Explain SQL injection with any tool

Use sqlmap, an automated tool that detects and exploits SQL injection flaws to extract database information.

## 7. Explain difference between VA and PT

VA (Vulnerability Assessment) identifies potential vulnerabilities. PT (Penetration Testing) exploits them to assess impact.

## 8. How to write vulnerability assessment Report

Include Executive Summary, Scope, Methodology, Findings (with risk rating), Recommendations, and Conclusion.