Name: Aamir Hussain **CMS:023-22-0080**

Task 1: Define and Provide Examples for Various Network Attacks

1. Denial of Service (DoS) Attack

Definition: A DoS attack attempts to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

Example: An attacker floods a website with so many requests that it crashes and becomes inaccessible to users.

---

2. Man-in-the-Middle (MITM) Attack

Definition: In MITM attacks, an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.

Example: On a public Wi-Fi network, an attacker intercepts and reads login credentials sent to a banking website.

---

3. Phishing

Definition: A cyberattack that uses disguised emails or messages to trick users into revealing sensitive information like usernames, passwords, or credit card numbers.

Example: A fake email that looks like it's from PayPal asks the user to verify their account by clicking a malicious link.

---

4. Malware

Definition: Malware refers to any malicious software designed to damage, disrupt, or gain unauthorized access to a computer system.

Example: A user downloads a free video player from an untrusted site, which installs ransomware that locks their files and demands payment.

---

5. SQL Injection

Definition: A code injection technique that exploits a vulnerability in an application's software by injecting malicious SQL queries through user input.

Example: On a login form, an attacker enters ' OR '1'='1 in the username field, tricking the database into granting access without valid credentials

---

6. Exploiting Software Vulnerabilities

Definition: Attackers exploit bugs or flaws in software to execute unauthorized actions on a system.

Example: A hacker exploits a buffer overflow vulnerability in a web server to gain remote code execution and take control of the system.

---

7. Credential Stuffing

Definition: A type of cyberattack where attackers use stolen username-password combinations from previous data breaches to try and gain access to user accounts.

Example: An attacker uses a list of leaked Netflix login credentials on other websites like Amazon or Facebook hoping users reused the same passwords.

Name: Aamir Hussain **CMS:023-22-0080**

Task 2: Understand and Apply Defense Strategies

1. Firewalls

Purpose: Monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Example: A company uses a firewall to block access to unauthorized ports and applications, reducing the risk of malware infections.

---

2. Intrusion Detection and Prevention Systems (IDPS)

Purpose: Detects and potentially blocks intrusions by monitoring network traffic for suspicious activity.

Example: An IDPS identifies and alerts administrators about a potential brute-force login attempt on the company's email server.

---

3. Antivirus and Anti-malware Software

Purpose: Detects, prevents, and removes malicious software.

Example: Antivirus software identifies and quarantines a trojan downloaded via a fake email attachment.

---

4. Encryption

Purpose: Ensures that data is only readable to intended recipients by converting it into an unreadable format without a decryption key.

Example: A user's connection to their bank is protected by HTTPS, encrypting data such as credit card numbers.

---

5. Authentication Mechanisms

Purpose: Verifies the identity of users before granting access to systems.

Example: Multi-Factor Authentication (MFA) adds a second layer of protection, such as a one-time code sent to a mobile phone.

---

6. Security Patches and Updates

Purpose: Fix known vulnerabilities in operating systems and applications.

Example: Microsoft releases a patch for a critical Windows vulnerability; organizations must apply it to avoid exploits like WannaCry.

---

7. Security Awareness Training

Purpose: Educates employees about cybersecurity threats and how to avoid them.

Example: A company conducts monthly training to help employees identify phishing emails and avoid clicking on suspicious links.

---

8. Network Segmentation

Purpose: Divides the network into segments to contain attacks and limit lateral movement.

Example: A company isolates its finance servers on a separate VLAN to protect them from attacks targeting the general network.

The End!