**B. TECH(Hons.) CSE-CSCQ**

**2nd Year**

**Quantum University**

**Assignment**

**(Morning Assignment)**

**Question 1. What is IPSEC?**

**Answer 1.**

IPsec (Internet Protocol Security) is a suite of protocols and algorithms for securing data transmitted over the internet or any public network. The Internet Engineering Task Force, or IETF, developed the IPsec protocols in the mid-1990s to provide security at the IP layer through authentication and encryption of IP network packets.

IPsec originally defined two protocols for securing IP packets: Authentication Header (AH) and Encapsulating Security Payload (ESP). The former provides data integrity and anti-replay services, and the latter encrypts and authenticates data.

The IPsec suite also includes Internet Key Exchange (IKE), which is used to generate shared security keys to establish a security association (SA). SAs are needed for the encryption and decryption processes to negotiate a security level between two entities. A special router or firewall that sits between two networks usually handles the SA negotiation process.

**Question 2. What is DNSSEC?**

**Answer 2.**

DNSSEC is a suite of extensions that improve Domain Name System (DNS) security by verifying that DNS results have not been tampered with. Enterprises can use DNSSEC to improve their DNS security.

DNS technology wasn’t designed with security in mind. One example of an attack on DNS infrastructure is DNS spoofing. An attacked hijacks a DNS resolver’s cache, causing users who visit a website to receive an incorrect IP address, and view an attacker’s malicious site instead of the site they intended.

**Question 3. What is DNS spoofing?**

**Answer 3.**

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user’s computer, giving the perpetrator long-term access to it and the data it stores.

Methods for executing a DNS spoofing attack include:

* **Man, in the middle (MITM)** – The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.
* **DNS server compromise** – The direct hijacking of a DNS server, which is configured to return a malicious IP address.

**Question 4. Explain DOS attack?**

**Answer 4.**

Denial of service attack (DOS) is an attack against computer or network which reduces, restricts or prevents accessibility of its system resources to authorized users.

Distributed Denial of Service (DDoS) attack is an attack where multiple compromised systems simultaneously attack a single system; thereby, causing a DOS attack for the users of the target.

An attacker can select the Zombies randomly or topologically and once compromised, he sets up a command and controller to control the zombies that attack the target. A bot is a malicious software installed on compromised machines; this gives the attacker control over the zombies. The network of Bots is called botnet.