ASSIGNMENT-1

CYBER ATTACKS

1.**Malware Attack**: Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.It executes unauthorized actions on the victim's system. The malicious software (a.k.a. virus) encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.

2.**Phishing Attack:** Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.

3. **Password Attack**: Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking of passwords. The attacker uses various techniques to access and expose the credentials of a legitimate user, assuming their identity and privileges

4. **Man-in-the-Middle Attack**: A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other

5. **SQL Injection Attack:** SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

6. **Denial-of-Service Attack**: A denial-of-service (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them.

7. **DNS Spoofing**: It is a type of security hacking that corrupts the Domain name system. The attacker presents fake data to the DNS cache. DNS cache in turn makes the server return an incorrect IP address. The DNS spoofing helps the attacker to divert traffic to the false website placed by the attacker.

samhitha

ASSIGNMENT-1