Task 5

1. **Dos/DDoS -**

Denial of Service where an attacker attacks by sending numerous service request packets overwhelming the servicing capability of the web server, resulting in crashing and unavailability for the users.

1. **DNS Server Hijacking -**

DNS Server Hijacking, is also known as DNS redirection, where an attacker modifies DNS configurations. DNS redirection's primary use is pharming, where attackers display unwanted ads to generate some revenue, and Phishing--where attackers show fake websites to steal credentials.

1. **DNS Amplification Attack -**

A DNS Amplification Attack happens when an attacker spoofs the lookup request to the DNS Server with the DNS recursive method. The size of the requests results in a Denial of Service attack.

1. **Directory Traversal Attacks -**

Directory traversal, also is known as Path Traversal, is an HTTP attack that allows attackers to access restricted directories and reveal sensitive information about the system using dot and slash sequences.

1. **Man in the Middle Attack -**

A Man in the Middle / Sniffing attack happens when an attacker positions himself between a user and the application to sniff the packets. The attacker's goal is to steal sensitive information such as login credentials, credit card details, etc.

1. **Phishing Attacks -**

A Phishing attack is a social engineering attack to obtain sensitive, confidential information such as usernames, passwords, credit card numbers, etc. It is a practice of fraudulent attempts that appear to come from a reputable source. Scammers mostly use emails and text messages to trick you in a phishing attack.

1. **Website Defacement -**

Website Defacement is an attack where an attacker changes the website/web page's visual appearance with their messages. SQL injection attack is mainly used in web defacement. An attacker can add SQL strings to craft a query maliciously and exploit the webserver.

1. **Web Server Misconfiguration -**

Web Server Misconfiguration is when unnecessary services are enabled, and default configurations are being used. The attacker may identify weaknesses in terms of remote functions or default certifications, and can exploit them. An attacker can easily compromise systems by some attacks such as SQL Injection, Command Injection.

1. **HTTP Response Splitting Attacks -**

HTTP Response Splitting is a straightforward attack when the attacker sends a splitting request to the server, which results in the splitting of a response into two responses by the server. The second response is in the hand of the attacker and is easily redirected to the malicious website.

1. **SSH Brute Force Attacks -**

Brute force is where an attacker uses trial and error to guess login info by submitting many passwords or paraphrases. In an SSH Brute force attack, the intruder brute forces the SSH tunnel to use an encrypted tunnel. The encrypted tunnel is for communicating between the hosts. Hence, the attacker gains unauthorized access to the tunnel.