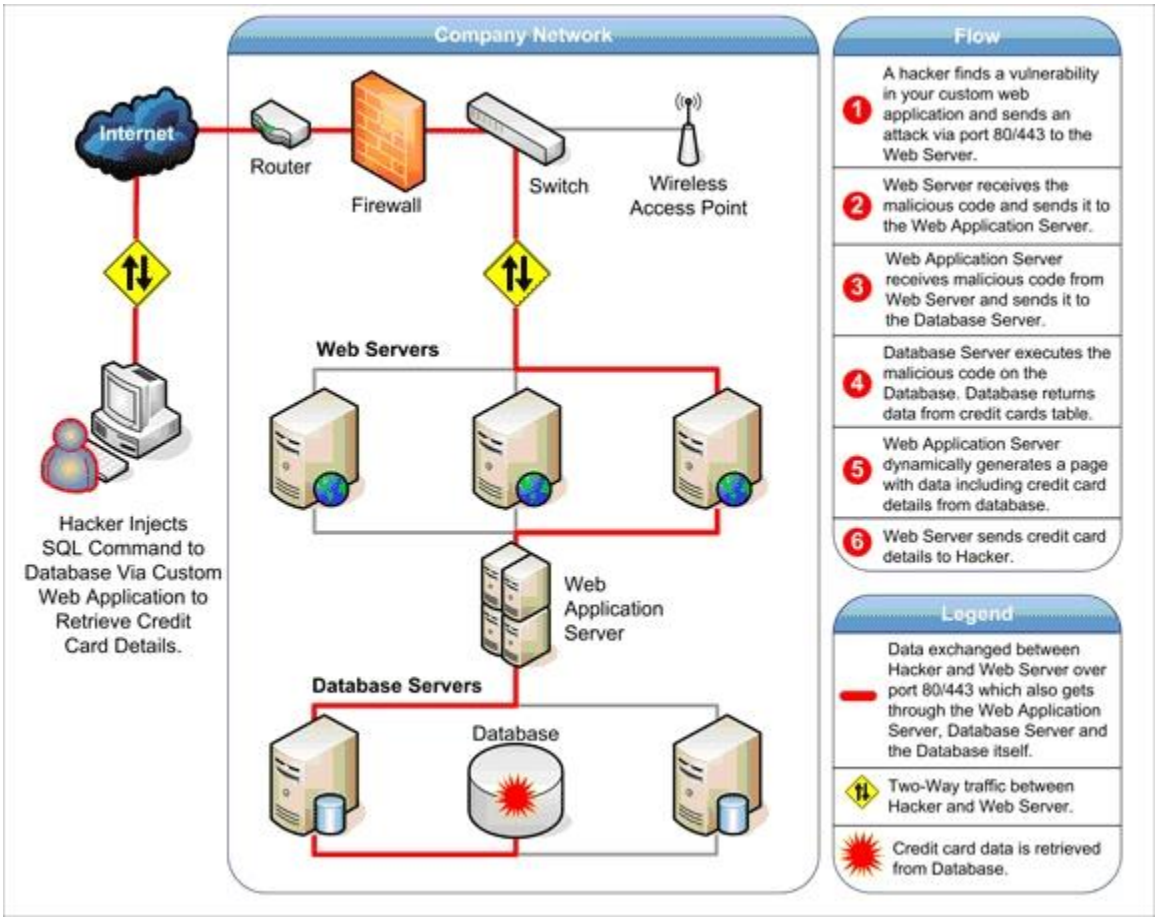
Task – 5

Name : C DEVAKI NANDAN REDDY

Explain any 10 Web Server Attacks determine them using images if Available



Web Server and its Types of Attacks

- Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)
- Web Defacement Attack
- SSH Brute Force Attack
- Cross-site scripting (XSS)
- Directory Traversal

- DNS Server Hijacking
- MITM Attack
- HTTP Response Splitting Attack

1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OF-SERVICE (DDOS): Denial of Service is when an internet hacker causes the web to provide a response to a large number of requests. This causes the server to slow down or crash and users authorized to use the server will be denied service or access. Government services, credit card companies under large corporations are common victims of this type of attack

2. WEB DEFACEMENT ATTACK: In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim. The attackers hack into a web server and replace a website hosted with one of their own.

3. SSH BRUTE FORCE ATTACK: By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access. This exploit can be used to send malicious files without being noticed. Unlike a lot of other tactics used by hackers, brute force attacks aren't reliant on existing vulnerabilities

4. CROSS SITE SCRIPTING (XSS): This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.

5. DIRECTORY TRAVERSAL: Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration. The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.

6. DNS SERVER HIJACKING: DNS Hijacking refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up. DNS Redirection is another name for this.

7. MITM ATTACK: Man-in-the-Middle (MITM) attack allows the attacker to access sensitive information by blocking and modifying the connection between the end-user and web servers. In MITM attacks or smells, the hacker captures or corrects modified messages between the user and the web server by listening or intervening in the connection. This allows the attacker to steal sensitive user information such as online banking details, usernames, passwords, etc., which

are transmitted online to the webserver. The attacker entices the victim to attach to an Internet server by pretending to be an agent.

8. HTTP RESPONSE SPLITTING ATTACK: HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering. Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data, it works just as well with HTTPS. The attack can be carried out in a variety of ways.

HOW TO PREVENT THESE ATTACKS :

- **Keep your system up to date:** Not updating the software regularly makes it weaker and leaves the system more vulnerable to attacks. Hackers take advantage of these flaws, and cybercriminals take advantage of them to get access to your network.
- **Prevent connecting to the public WiFi network:** An unsecured Wi-Fi connection can be used by hackers to spread malware. If you allow file-sharing across a network, a hacker can simply infect your computer with tainted software. The ability of a hacker to put himself between you and the connection point poses the greatest threat to free Wi-Fi security.
- **Install Anti-virus, and update it regularly:** Antivirus software is designed to identify, block, and respond to dangerous software, such as viruses, on your computer. Because computers are continuously threatened by new viruses, it is critical to keep antivirus software up to date. Anti-virus updates include the most recent files required to combat new threats and safeguard your machine. These signature files are provided on a daily basis, if not more frequently.
- **Use IDS and firewall with updated signatures:** NIDS are security threat detection and prevention systems that identify and prevent security threats from infiltrating secure networks. The use of NIDS has a negligible effect on network performance. NIDS are typically passive devices that listen to a network without interfering with the network's normal operation.
- **Backup your data:** The fundamental purpose of a data backup is to keep a safe archive of your vital information, whether it's classified

documents for your business or priceless family photos so that you can quickly and effortlessly recover your device in the event of data loss. Backup copies allow data to be restored from a previous point in time, which can aid in the recovery of a business after an unanticipated occurrence. Protecting against primary data loss or corruption requires storing a copy of the data on a secondary medium.

- **Install a Firewall:** Firewalls defend your computer or network from outside cyber attackers by filtering out dangerous or superfluous network traffic. Firewalls can also prevent harmful malware from gaining internet access to a machine or network.