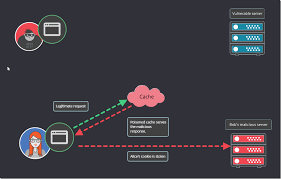
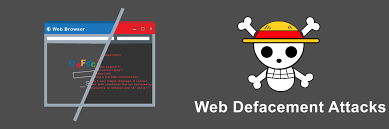
**Task -5**

**Top 10 Web Server based attacks-Tuesday (29-08-23) by Sameer Chauhan**

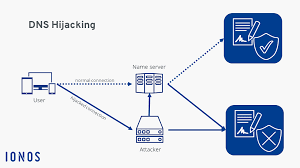
**1-Http Response-splitting attack-HTTP response splitting is a web security vulnerability that occurs when an attacker is able to inject malicious characters into HTTP response headers, potentially leading to various forms of attacks**.

****

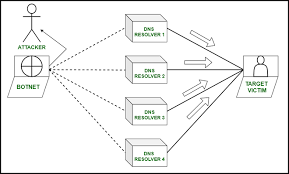
**2-web defacement-Web defacement is a type of cyber attack in which an attacker gains unauthorized access to a website and alters its visual appearance by replacing or modifying its content. The goal of a web defacement attack is to deface the website's pages, often by replacing legitimate content with the attacker's own messages, images, or political statements**.

****

**3-DNS server hijacking-In this type of attack the attacker compromises the dns of a server and alter its settings and redirect user to a malicious website.**

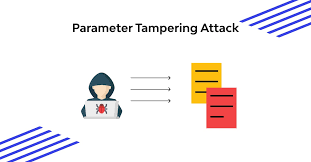
****

**4-Dns amplification attack-it is a type of D -DOS attack which exploit the vulnerability of a dns servers to turn initially small queries into much larger payloads, which are used to bring down the victim's servers.**

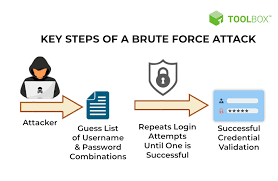
****

**5-Form tempering/web parameter attack-**

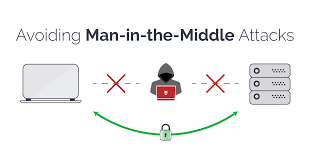
***Parameter tampering is a type of web-based cyber attack in which certain parameters in a URL are changed without a user's authorization. In some cases, the data entered by a user into a form field of a webpage may also be modified -- again, without the user's authorization.***

****

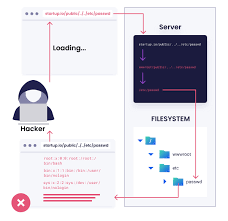
**6-SSH brute force attack-it means hacking secure shell accounts by guessing passwords,user id by guessing methods or using tools like burp suite to peform automatic brute force attacks**

****

**7-MITM-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,**

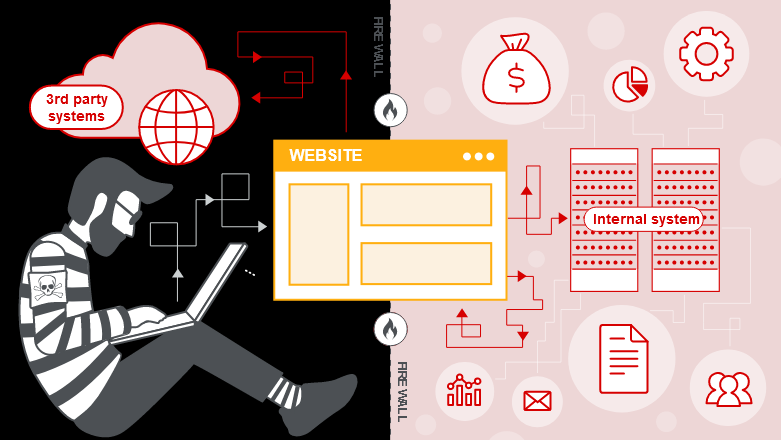
****

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

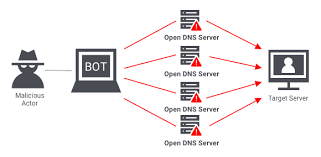
****

**9-Server Side Request forgery-Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.**

**In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials.**



**10-D/D-DOS ATTACK-A DoS (denial-of-service) attack is a cyberattack that makes a computer or other device unavailable to its intended users. This is usually accomplished by overwhelming the targeted machine with requests until normal traffic can no longer be processed**

****