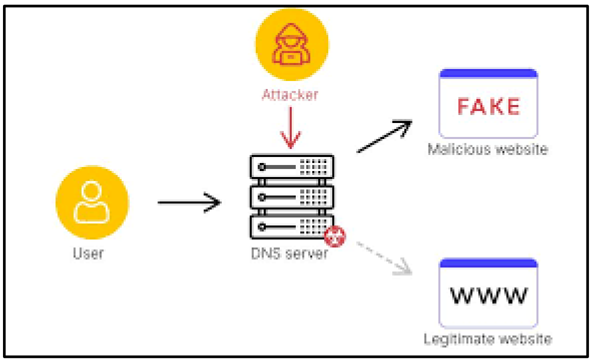
AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-5: 10 Web server attacks

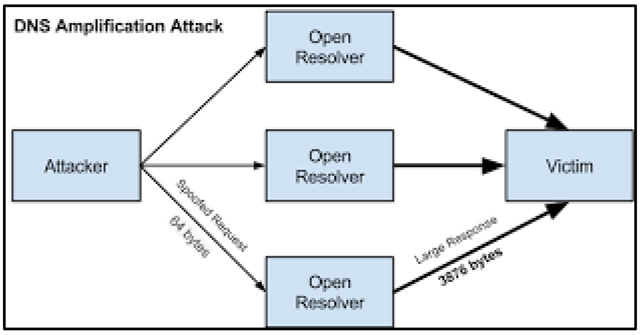
1. DNS Server Hijacking:

Domain Name Server (DNS) hijacking, also named DNS redirection, is a type of DNS attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites. To perform the attack, perpetrators either install malware on user computers, take over routers, or intercept or hack DNS communication.



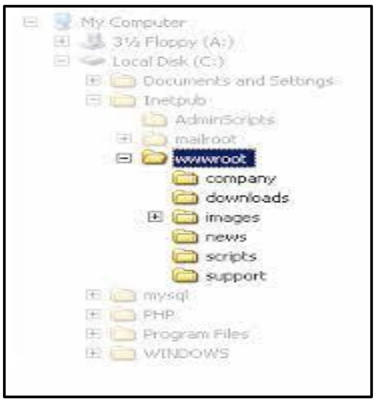
2. DNS Amplification Attack:

This attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.

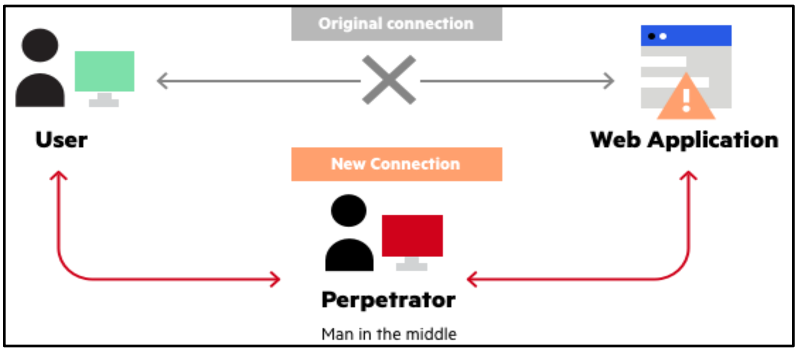


3. Directory Traversal Attacks:

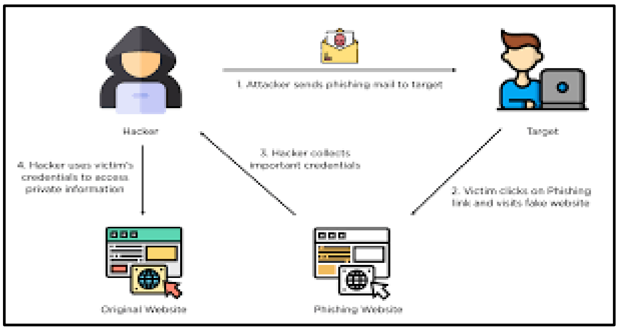
Directory traversal is a type of HTTP exploit in which a hacker uses the software on a web server to access data in a directory other than the server's root directory. If the attempt is successful, the threat actor can view restricted files or execute commands on the server.



4. Man in the Middle Attack:
A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications where logging in is required.

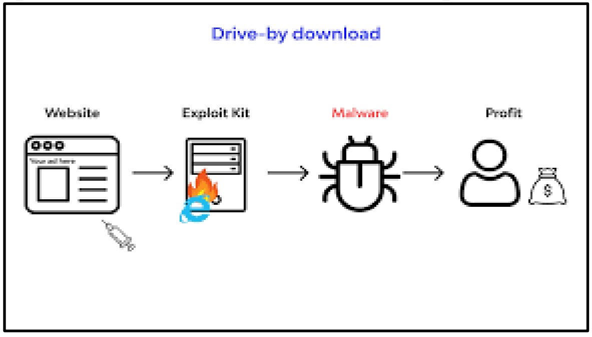


5. Phishing Attacks:
A Phishing attack is a social engineering attack to obtain sensitive, confidential information such as usernames, passwords, credit card numbers, etc. These are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.



1. Attacker sends phishing mail to target
Hacker
Target
3. Hacker collects important credentials
4. Hacker uses victim's credentials to access private information
2. Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

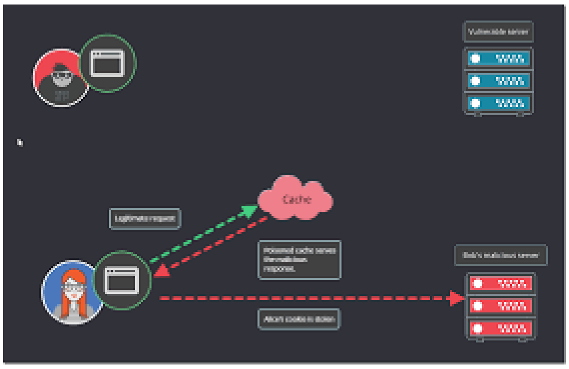
6. Drive-by download:
A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats. Cybercriminals make use of drive-by downloads to steal and collect personal information, inject banking Trojans, or introduce exploit kits or other malware to endpoints, among many others.



,

7. Web Server Misconfiguration:
Security misconfiguration is a common issue in organizations that occurs when a server or web application is not configured correctly, leaving vulnerabilities that can potentially be spotted by attackers leading to server misconfiguration attacks.

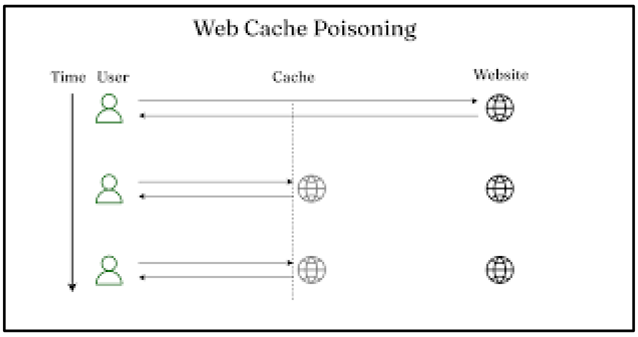
8. HTTP Response Splitting Attacks:
HTTP response splitting is a form of web application vulnerability, resulting from the failure of the application or its environment to properly sanitize input values. It can be used to perform cross-site scripting attacks, cross-user defacement, web cache poisoning, and similar exploits.



9. SSH Brute Force Attacks:
Brute force is where an attacker uses trial and error to guess login info by submitting many passwords or paraphrases. An SSH brute force attack is a hacking technique that involves repeatedly trying different username and password combinations until the attacker gains access to the remote server. The attacker uses automated tools that can try thousands of username and password combinations in a matter of seconds, making it a fast and effective way to compromise a server.

10. Web cache poisoning attack:
Web cache poisoning is an advanced technique whereby an attacker exploits the behavior of a web server and cache so that a harmful HTTP response is served to other users. It involves two phases. First, the attacker must work out how to elicit a response from the back-end server that inadvertently contains some kind of dangerous payload. Once successful, they

need to make sure that their response is cached and subsequently served to the intended victims.


Web Cache Poisoning
Time
User
Cache
Website