UNIT 2
Understanding DoS and DDoS Attacks, Sniffers, and Session Hijacking in Web Application Security

Web application security

- **Web application security is a critical aspect of the digital world.**
- **It ensures the protection of sensitive data and maintains the integrity of online services.**
- **One of the major concerns in web application security is the threat of denial of-service (DoS) and distributed denial-of-service (DDoS) attacks, sniffers, and session hijacking.**

1.1 What are DoS and DDoS Attacks?

- A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
- A DoS attack generally consists of efforts to temporarily interrupt or suspend services of a host connected to the Internet.
- Distributed denial-of-service attacks are sent by two or more people, or bots, and
- Denial-of-service attacks are sent by one person or system.

Symptoms of DoS Attacks

- **Unusually slow network performance (opening files or accessing websites)**
- **Unavailability of a particular website Inability to access any website**
- **Dramatic increase in the number of spam emails received (email bomb)**
- **Disconnection of a wireless or wired internet connection.**
- In the case of a wired connection, such as Ethernet, the attacker may flood the network with excessive traffic, causing switches, routers, or other network devices to become overloaded. This overload can lead to network congestion, packet loss, and ultimately the disconnection of the wired connection from the network.
- **Long-term denial of access to the web or any internet services**

How to protect against DoS attacks

- Firewalls: Imagine a firewall as a **security guard** for your network. It looks at all the traffic **coming in and going out** and decides **what's allowed and what's not.**
- By setting up strict rules, you can tell the firewall to block any suspicious or harmful traffic while letting the good stuff through.
- **Switches and routers:** These are like **traffic controllers** for your network. You can **configure them** to control how much data is allowed to flow through at once.
- Intrusion Prevention Systems (IPS): Think of an IPS as a system that's trained to recognize specific signs of a DoS attack. When it sees those signs, it jumps into action.
- Traffic analysis tools and network monitoring: These are like security cameras for your network.

They watch the traffic in real-time, looking for anything suspicious. If they spot something, they alert you so you can take action to stop the attack.

Incident response

- Incident response is the process of managing and mitigating the effects of security incidents or attacks.
- It involves a set of predefined steps and procedures to detect, contain, eradicate, and recover from security breaches in a timely and effective manner.
- steps involved in an incident response plan is:
- **1. Preparation:** This phase involves establishing an incident response team and defining their roles and responsibilities. The team should include representatives from IT, security, legal, and other relevant departments. Regular training and exercises should also be conducted to ensure that the team is prepared to respond effectively to incidents.

2. Detection and Analysis: The next step in responding to a security incident is detecting it. This may involve monitoring network traffic or using intrusion detection systems (IDS) to identify suspicious activity.

Once an incident is detected, it needs to be analyzed to determine the nature and scope of the att ques and tactics.

A log file is like a diary or journal for a computer system. It keeps a record of all the important events and actions that happen on the system over time. These events can include things like:

3. Containment: After the incident has been analyzed, the next step is to contain it to prevent further damage.

This may involve isolating affected systems from the network, blocking malicious traffic, or disabling user accounts.

The goal is to minimize the impact of the incident and prevent it from spreading to other parts of the organization's infrastructure.

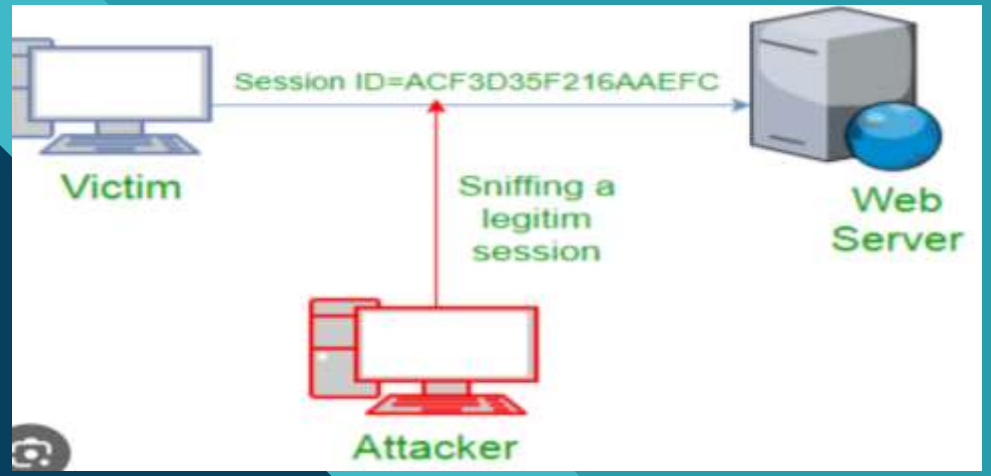
4. Eradication: Once the incident has been contained, the next step is to eradicate the root cause of the problem.

This may involve removing malware from infected systems, patching vulnerabilities, or implementing additional security controls to prevent similar incidents from occurring in the future.

5. Recovery: After the threat has been neutralized, the organization can begin the process of restoring affected systems and services. This may involve restoring data from backups, rebuilding compromised systems, or implementing additional security measures to enhance resilience against future attacks.

6. Post-Incident Analysis: After everything's back in order, they take a good look at what happened. They figure out what went wrong, what they did right, and how they can do better next time. It's like reviewing the plan, and mistakes, and how to avoid such mistakes

SNIFFERS



- also known as packet analyzers or protocol analyzers.
- Sniffers are tools that intercept and analyze network traffic.

GOOD (ETHICAL) USES OF SNIFFERS:

Network Troubleshooting: Sniffers can be used by network administrators to troubleshoot network issues.

By analyzing network traffic, they can identify bottlenecks, misconfigurations, or faulty devices affecting network performance.

Why do hackers use packet sniffers?

- Hackers use packet sniffing attacks for many reasons, such as recording your online activities, reading your emails, and viewing your passwords and banking details.
- data is captured at the packet level, in its raw form, containing zeros and ones – binary digits

Types of Sniffers

- **Passive Sniffers:** These sniffers only capture and display packets without interacting with them. They can be used to monitor network traffic and analyze network performance.

- **Active Sniffers:** These sniffers can inject packets into the network or modify existing packets, allowing them to perform more advanced tasks such as hijacking sessions or launching attacks.

- **Protocol-Specific Sniffers:** Some sniffers are designed to analyze specific network protocols, such as HTTP, FTP, or SNMP, providing a more focused view of network activity.
- **Example – Fiddler.**

protect against sniffer attacks:

- To protect against sniffer attacks, organizations should implement the following countermeasures:

- 1. Use encryption, such as SSL/TLS, to secure data transmitted over the network.
- 2. Strong authentication mechanisms, such as two-factor authentication, to protect against eavesdropping and unauthorized access.
- 3. Regularly update network devices and software
- 4. Implement access control.

Session Hijacking

- Session hijacking, also known as cookie hijacking, is the exploitation of a

valid computer session to gain unauthorized access to information or services in a computer system.

- Imagine you're using a website, and you log in with your username and password. After you log in, the website gives you a special code (called a session token) to show that you're authorized to use the site.
- This code is like a ticket that lets you do things on the website, like posting comments or shopping.
- Now, AN ATTACKER wants to use your account without your permission.
- They could try to steal this special code (session token) to pretend they're you. This is called session hijacking.

Methods of Session Hijacking

- **1. Session fixation: In a session fixation attack, an attacker aims to fixate or control a user's session identifier, such as a session cookie or URL parameter, to gain unauthorized access to the user's account.**

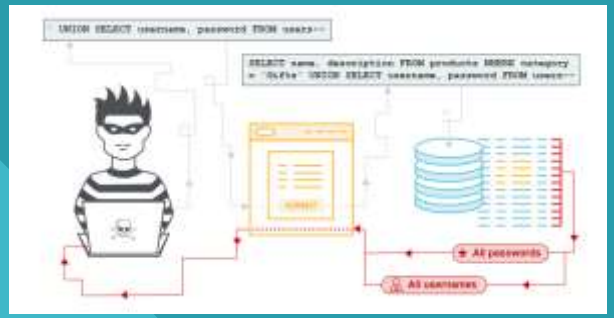
1. **Initial Access: The attacker begins by accessing the target website or application that uses session identifiers for authentication, such as an online banking site.**
2. **Session Initiation: The attacker initiates a session with the website, receiving a temporary session identifier from the server.**
3. **Session Fixation: The attacker creates a link containing the session identifier obtained in step 2 and sends it to the victim, TRICKING them to click on it. This link could be embedded in an email, social media message, or any other form of communication.**
4. **Victim Interaction: The victim clicks on the link sent by the attacker, unknowingly using the session identifier provided by the attacker to authenticate with the website.**
5. **Exploitation: With the victim's session now associated with the attacker's identifier, the attacker can access the victim's account, without authentication. They may then perform various malicious activities, such as transferring funds in the case of a banking website, changing account settings, or accessing sensitive information.**
6. **Maintaining Access: The attacker may continue to exploit the compromised session for as**

- **2. Physical access:** When you log in to a website or application, the server generates a session token for you. This token is stored temporarily in the server's memory.
- The server keeps track of which token belongs to which user so that it can recognize you when you make more requests.
- **3. File Storage:** Sometimes, especially for more complex systems or when sessions need to last longer than just the current session, session tokens are stored in files on the server's hard drive. These files contain information about your session, including your session token.
- 3. Why is it Vulnerable?
- If someone gets physical access to the server where these session tokens are stored, they could potentially steal them.
- Memory Access: If an attacker gains access to the server's memory, they could find the session token associated with your session.
- File Access: Similarly, if they can access the files where session tokens are stored, they could retrieve them from there.
-

Mitigating the Risk To prevent this, developers and system administrators implement security measures:

- **Encryption**: (SSL/TLS) Session tokens should be encrypted when stored, making them unreadable even if someone gains access to them.
- **Access Controls**: Limiting physical access to the server.
- **Regular Security Checks**: Periodic audits and checks help identify vulnerabilities that could be exploited by attackers.
- **Token Lifespan**: Session tokens should have a limited lifespan, expiring after a certain period of inactivity or when the user logs out.
- Encourage users to log out of websites when they are finished using them to reduce the risk of session hijacking

Common Web Application Vulnerabilities



What is SQL injection (SQLi)?

- Attackers insert malicious SQL code into user-input fields, allowing them to manipulate the database and access sensitive information.
- This can allow an attacker to view data that they are not normally able to retrieve.
- This might include data that belongs to other users.
- A successful SQL injection attack can Insert/Update/Delete database data, execute administration operations on the database (such as shutdown the DBMS), get the content of a given file present on the DBMS.
- Imagine you're filling out a form on a website, like a login page. When you type something into that form, the website needs to store or retrieve that information from a database.
- Now, if the website isn't properly secured, hackers can sneakily inject their own malicious SQL (Structured Query Language) commands into those forms instead of normal data.