جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الأمن السيبراني

Lecture: 7

Denial of Service (DoS)

Subject: software security

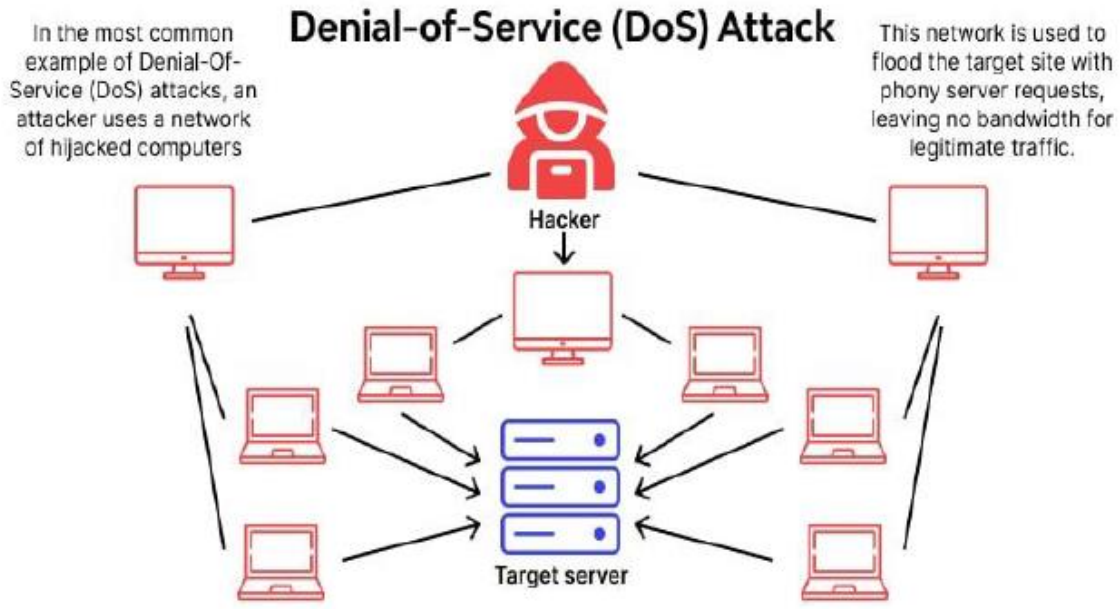
second Stage

Lecturer: Asst. Lecturer. Suha Alhussieny

Denial of Service (DoS)

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.

A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

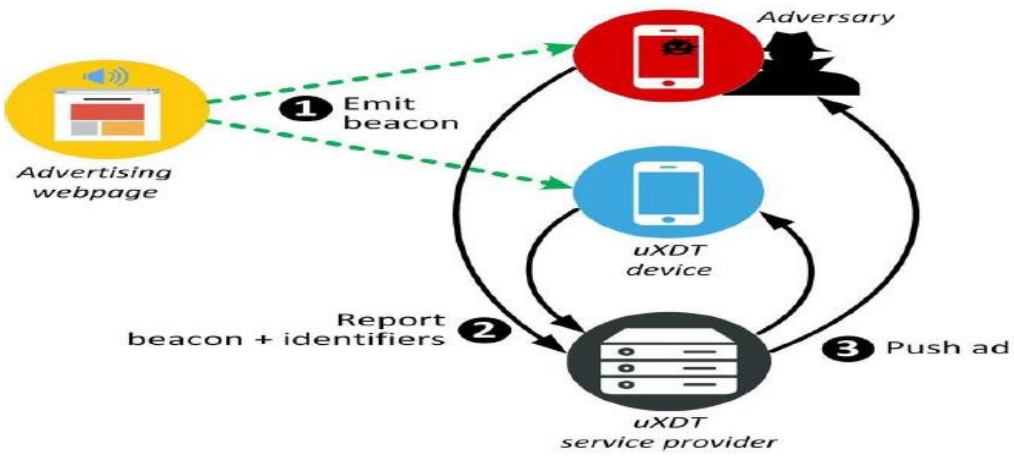


Information Leakage

Information leakage is the sharing of sensitive information with unauthorized parties. The leakage can be either;

1. Accidental, such as an employee sharing confidential information with an external party via email, or malicious, such as the exfiltration of data through phishing scams.
2. Regardless of the intent, however, the information shared is valuable to hackers and can be used to execute attacks on your organization's infrastructure, services or applications.

While information leaks originate from within an organization, data breaches are a result of actions that take place from unauthorized users from outside of the organization. Encryption, implementing security controls and classifying sensitive data are all strategies organizations use to prevent data loss. In addition, many organizations have various data leak prevention strategies and technology in place to defend against data breaches.

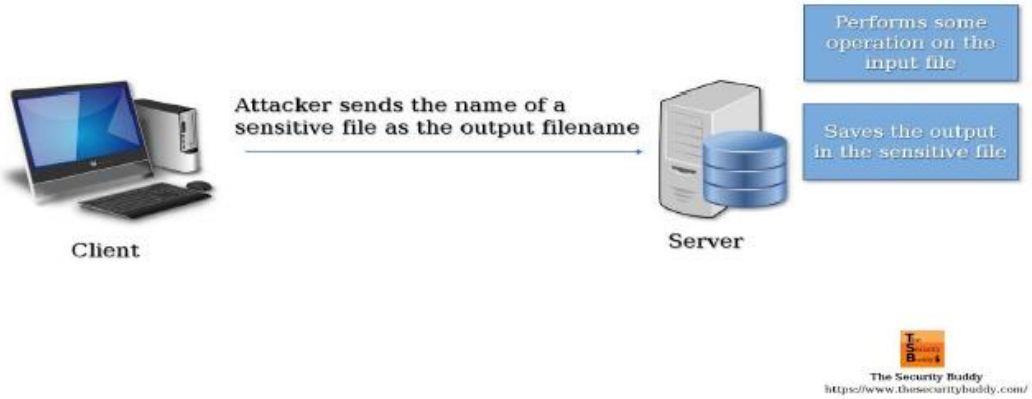


Confused Deputy

The "Confused Deputy" problem is a security issue that arises when a program (the "deputy") is tricked into performing actions on behalf of an attacker with more privileges than the attacker should have. This problem often occurs in systems where one program (the deputy) performs tasks on behalf of another program or user, and the deputy is tricked into executing actions it would not normally perform.

Here's a simplified example of how the Confused Deputy problem might manifest:

1. **Scenario**: Imagine a web application that allows users to upload files. The application processes these files on behalf of users, using a server-side script with permissions to read and write files in a specific directory.
2. **Exploitation**: An attacker might upload a file with a name that includes a path traversal attack (e.g., ../sensitive_file.txt). The application's script, operating with the server's higher privileges, might process this file and inadvertently read or write to sensitive files outside the intended directory.
3. **Result**: The attacker successfully accesses or modifies sensitive files by exploiting the higher privileges of the server-side script.



Privilege Escalation

Privilege escalation is a type of security vulnerability where an attacker gains elevated access to resources or permissions beyond what they are normally authorized to have. This can occur through various methods, leading to unauthorized access to sensitive data, system control, or administrative functions. Privilege escalation can be categorized into two main types:

Vertical privilege escalation occurs when a user with lower-level permissions gains access to higher-level privileges or administrative rights. For example:

- **Exploiting Vulnerabilities**: Attackers might exploit software vulnerabilities to gain administrative access. For instance, vulnerability in an application might allow a user to execute

commands with root privileges.

- **Weak Authentication**: Weak or misconfigured authentication mechanisms can allow an attacker to impersonate an administrative user and gain elevated access.

- **Misconfigured Permissions**: Incorrectly configured file or directory permissions can enable a user to access or modify files they shouldn't.

Horizontal privilege escalation happens when a user gains access to resources or permissions of another user with the same level of privilege. For example:

- **Session Fixation**: An attacker might hijack a user's session to access resources that the user can access, even though the attacker shouldn't have access to those resources.
- **Insecure APIs**: APIs that do not enforce proper access controls may allow an attacker to perform actions intended for other users with similar permissions.