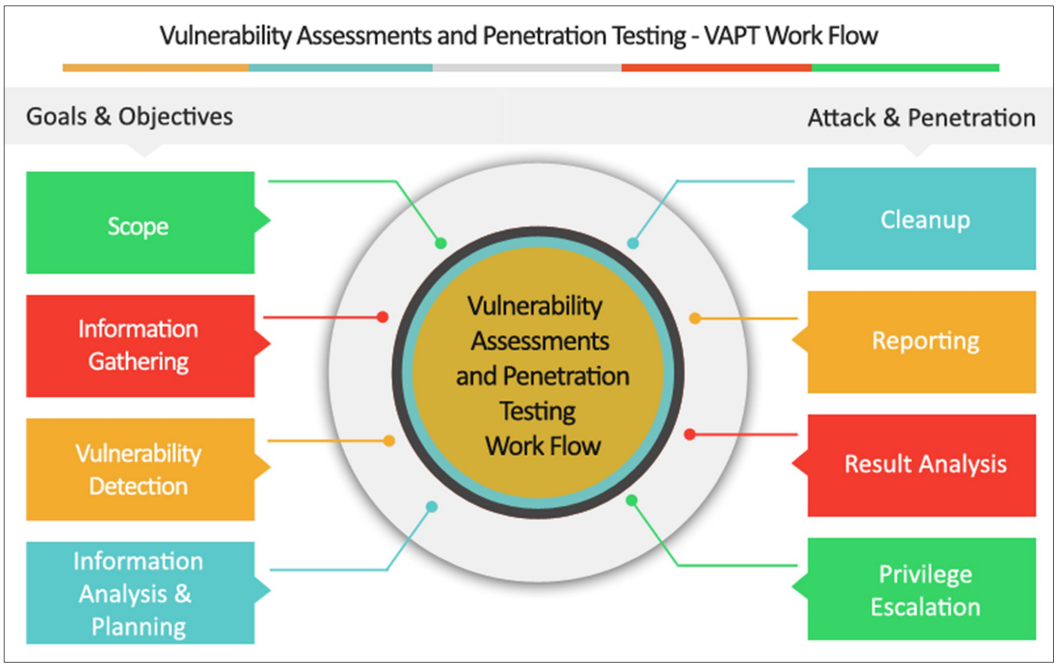
UNIT-II Web Application Security Vulnerability Terminology

VULNERABILITY ASSESSMENT is a process to evaluate the security risks in the software system in order to reduce the probability of a threat. It is also called Vulnerability Testing.

A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of the system's security policy. The **purpose** of Vulnerability Assessment is to reduce the possibility for intruders (hackers) to get unauthorized access. Vulnerability Analysis depends upon two mechanisms namely Vulnerability Assessment and Penetration Testing (VAPT).

- VAPT is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

Vulnerability Assessment and Penetration Testing (VAPT) Process



Vulnerability Assessment and Penetration Testing (VAPT) Process

Goals& Objectives: – Defines goals and objectives of Vulnerability Analysis

1. **Scope**: – While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.
   The following are the three possible scopes exist:

- Black Box Testing: – Testing from an external network with no prior knowledge of the internal network and systems.
- Grey Box Testing: – Testing from either external or internal networks, with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- White Box Testing: – Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

2. **Information Gathering**: – Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing, and White Box Testing
3. **Vulnerability Detection**: -In this process, vulnerability scanners are used, it will scan the IT environment and will identify the vulnerabilities.
4. **Information Analysis and Planning**: – It will analyse the identified vulnerabilities, to devise a plan for penetrating into the network and systems.
5. **Reporting**
6. **Remediation**
   - The process of fixing the vulnerabilities.
   - For every vulnerability

Types of a vulnerability scanner

1. Host Based
   - Identifies the issues in the host or the system.
   - The process is carried out by using host-based scanners and diagnose the vulnerabilities.
   - The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.
2. Network-Based
   - It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
   - This process is done by using Network-based Scanners.
3. Database-Based
   - It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: – Injecting SQL statements into the database by the malicious users, which can read the sensitive data's from a database and can update the data in the Database.)

Vulnerability Testing Methods

Active Testing

- Inactive Testing, a tester introduces new test data and analyzes the results.

- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.

- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive Testing

- Passive testing, monitoring the result of running software under test without introducing new test cases or data

Network Testing

Network Testing is the process of measuring and recording the current state of network operation over a period of time.
Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.
We need to Test the following Network Characteristics:-

- Utilization levels
- Number of Users
- Application Utilization

What is a False Positive in Cybersecurity?

When a piece of security equipment warns you of a problem, this is known as a false positive. The problem is that the security device is malfunctioning. This is a positive. However, it's a false positive, meaning there was no issue.

These warnings are based on signatures if you receive a message from an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). A piece of information that gone through the IPS that matches a signature and informs you that there was a match to that. In most cases, we have to rely on these signatures, so make sure you're using the most updated signatures to avoid false positives.

What is CWSS?

CWSS (Common Weakness Scoring System) is organized into three *metric groups*: Base Finding, Attack Surface, and Environmental. Each group contains multiple metrics - also known as *factors* - that are used to compute a CWSS score for a weakness.

- **Base Finding metric group**: captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls.
- **Attack Surface metric group**: the barriers that an attacker must overcome in order to exploit the weakness.
- **Environmental metric group**: characteristics of the weakness that are specific to a particular environment or operational context.

What is a CVE?

- CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw

that's been assigned a CVE ID number. Security advisories issued by vendors and researchers almost always mention at least one CVE ID.

STRIDE stands for (Spoofing+ Tampering +Repudiation +Information Disclosure +Denial of Service+ Elevation of Privilege.)

DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5. Calculation always produces a number between 10. Higher the number means more serious the risk is.