SECURITY TESTING:

Security Testing is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.

TYPES OF SECURITY TESTING:

Vulnerability Assessment (VA): This involves the use of automated tools to scan a system or application for known vulnerabilities and weaknesses. The goal is to identify potential entry points for attackers and assess the severity of each vulnerability.

TOOLS:

1. Astra Pentest
2. Intruder
3. Acunetix
4. Cobalt.IO
5. Burp Suite
6. Wireshark
7. Qualys Guard
8. Nessus
9. OpenVAS

Penetration Testing (Pen Testing): Penetration testing goes beyond vulnerability assessment by simulating real-world attacks to assess the security posture of a system. Ethical hackers, known as penetration testers or "white hat" hackers, attempt to exploit vulnerabilities and gain unauthorized access to the system to demonstrate its weaknesses.

TOOLS:

1. Kali Linux
2. nmap
3. Metasploit
4. Wireshark
5. John the Ripper
6. Hashcat
7. Hydra

Security Scanning: It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.

TOOLS:

1. NESSUS
2. OpenVAS
3. Nexpose
4. Burp Suite
5. OWASP ZAP
6. NIKTO
7. Retina

Risk Assessment: This testing involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High. This testing recommends controls and measures to reduce the risk.

TOOLS:

1 SpiraPlan by Inflectra
2 A1 Tracker

3 Risk Management Studio
4 Isometrix
5 Active Risk Manager
6 CheckIt
7 Isolocity
8 Enablon
9 GRC Cloud

Security Auditing: This is an internal inspection of Applications and Operating systems for security flaws. An audit can also be done via line by line inspection of code

TOOLS:

1. Nessus
2. Lynis
3. AIDE
4. Tripwire
5. OpenSCAP
6. OVAL

Ethical hacking: It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.

TOOLS:

1. Metasploit
2. NMAP
3. Nessus
4. Hydra
5. Gobuster
6. Netcat
7. Wireshark

Posture Assessment: This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

TOOLS:

1. Metasploit
2. NMAP

3.Nessus

4.Hydra

Application Security Testing (AST) : Application security testing describes methods organizations can use to find and eliminate vulnerabilities in software applications. These methods involve testing, analyzing, and reporting on the security posture of a software application throughout the software development lifecycle (SDLC).

The main goal of AST is to prevent software vulnerabilities before applications are released to the market, and failing that, quickly identify and remediate them in production. Successful AST results in more robust, secure source code, greater visibility over application security issues, and improved protection against internal and external threats.

TOOLS:

1.OWASP ZAP (Zed Attack Proxy)
2.Burp Suite
3.Acunetix
4.AppScan (IBM Security)
5.Checkmarx
6.Veracode
7.Qualys Web Application Scanner

Web Application Security Testing: The goal of web application security testing is to determine whether a web application is vulnerable to attack. It covers a variety of automatic and manual techniques.

Web application penetration testing aims to gather information about a web application, discover system vulnerabilities or flaws, investigate the success of exploiting these flaws or vulnerabilities, and evaluate the risk of web application vulnerabilities.

TOOLS:

1. OWASP ZAP
2. ACUNETIX
3. NETSPARKER
4. APPSCAN
5. W3af

API Security Testing: API security testing helps identify vulnerabilities in application programming interfaces (APIs) and web services, and assist developers in remediating those vulnerabilities. APIs provide access to sensitive data, and attackers can use them as an entry point to internal systems. Testing APIs rigorously and regularly can protect them from unauthorized access and abuse.

TOOLS:

1. Paw
2. Vrest
3. Apigee
4. Tricentis Tosca
5. Jmeter
6. HttpMaster

SDLC Phases	Security Processes
Requirements	Check for abuse/misuse incidents and do a security analysis.
Design	For designing, do a security risk analysis. Creating a test plan that includes security tests
Coding and Unit Testing	Security and Static and Dynamic Testing Testing in a White Box
Integration Testing	Black Box Testing

SDLC Phases	Security Processes
System Testing	Vulnerability scanning and black box testing
Implementation	Vulnerability Scanning, Penetration Testing
Support	Analyze the Impact of Patches