Software Testing

Static Testing	Software security analysis using automated tools. Do not analyze either the source code or the compiled application. Eg. Buffer overflow
Dynamic Testing	Analyze and test using running environment. Use to test software provided by third parties where no access to software code. Eg. cross-site scripting, SQL injection
Fuzz Testing	Type of dynamic testing which use specific inputs to detect flaws under stress/load. Eg. input invalid parameters to test
Mutation / Dumb Fuzzing	Using already modified input values to test.
Generational / Intelligent Fuzzing	Inputs models of expected inputs.
Misuse Case Testing	Evaluate the vulnerability of known risks and attacks.
Interface Testing	Evaluate performance of software modules against the interface specifications to validate working status.
Application Programming Interfaces (APIs)	Test APIs to verify web application meets all security requirements.
User Interfaces (UIs)	Includes graphic user interfaces (GUIs) and command-line interfaces (CLI). Review of user interfaces against requirement specifications.
Physical Interfaces	Eg. in physical machines such as ATM, card readers etc.
Unit Testing	Testing a small part of the system to test units are good for integration into final product.
Integration Level Testing	Transfer of data and control between program interfaces.
System Level Testing	Verify system has all the required specifications and functions.

Log Management System

OPSEC process	Analyze daily operations and review possible attacks to apply countermeasures.
Pen-test	Testing of network security in view of a hacker.
Port scanner	Check any port or port range open in a computer.
Ring zero	Internal code of the system.
Operational assurance	Verify software meets security requirements.
Supervisor mode	Processes running in internal protected ring.

Threat Assessment Modeling

STRIDE	Evaluate threats against applications or operating systems.
Spoofing	Use of false identity to gain access to system identity. Can use IP/ MAC address, usernames, wireless network SSIDs.
Tampering	Cause unauthorized modifications of data in transit or in storage. Results in violation of integrity as well as availability.
Repudiation	Deny an action or activity carried out by an attacker.
Information disclosure	Distribution of private/confidential or restricted information to unauthorized parties.
Elevation of privilege	Attack result in increase the level privileges for a limited user account.
Regular monitoring of key performance and risk indicators including	Number of open vulnerabilities and compromised accounts, vulnerability resolve time, number of detected software flaws etc.
Vulnerability scans	Automatically probe systems, applications, and networks.
TCP SYN Scanning	Sends a packet with SYN flag set. Also known as “half-open” scanning.
TCP Connect Scanning	Perform when a user running the scan does not have the necessary permissions to run a half-open scan.
TCP ACK Scanning	Sends a packet with the ACK flag set.
Xmas Scanning	Sends a packet with the FIN, PSH, and URG flags set.
Passive Scanning	Detect rogue scanning devices in wireless networks.
Authenticated scans	Read-only account to access configuration files.

Software Development Security Best Practices

WASC	Web Application Security Consortium
OWASP	Open Web Application Security Project
BSI	the Build Security In initiative
IEC	The International Electrotechnical Commission

Security Testing

To make sure security controls are properly applied and in use. Automated scans, vulnerability assessments and manual testing.

Software Threats

Viruses	Stealth virus • Polymorphic virus • Macro virus • • Spyware/Adware • Botnet • worm
Rootkit	Kernel-mode Rootkit • Bootkit • User-mode Rootkit • Virtual Rootkit • Firmware Rootkit
Source Code Issues	Buffer Overflow • Escalation of Privileges • Backdoor
Malware Protection	Antivirus software • Antimalware software • Security Policies

Considerations

- Resources availability
- Level of critical and sensitiveness of the system under testing
- Technical failures
- Control misconfigurations result in security loopholes
- Security attack risks
- Risk of performance changes
- Impact on normal operations

Verification & Validation

- Verification – SDLC design output meets requirements
- Validation – Test to ensure software meets requirements

Security Software

- Antimalware and Antivirus – Scan and log malware and virus detection
- IDS/IPS = Real time and promiscuous monitoring for attacks
- Network-based IDS
- Local network monitoring and passive and header level scanning .No host level scan.
- HOST BASED
- Monitor hosts using event logs
- Intrusion prevention system (IPS) – Attack detects and prevent
- Remote Access Software Should be access via a VPN
- Vulnerability assessment Software – should be updated and patched
- Routers – policy based access control

Logs

Network Flow	Network traffic capture
Audit logging	Events related to hardware device login and access
Network Time Protocol (NTP)	Should synchronize across entire network to have correct and consistent time in logs and device traffic flows.
Syslog	Device event message log standard.
Event types	Errors, Warnings, Information, Success Audits, Failure
Simple Network Management Protocol (SNMP)	Support for different devices such as Cisco.

Monitoring and auditing

Define a clipping level. A.K.A BASELINE

- Audit trails – event/transaction date/time, author /owner of the event
- Availability – Log archival
- Log Analysis – examine logs

Code Review and Testing

Person other than the code writer/developer check the code to find errors

Fagan inspections – steps	Planning • Overview • Preparation • Inspection • Rework • Follow-up
Code Coverage Report	Details of the tested code structure
Use cases	Percentage of the tested code against total cases
Code Review Report	Report create in manual code testing
Black-box testing	Test externally without testing internal structure
Dynamic Testing	Test code in run time
White-box testing	Detailed testing by accessing code and internal structure
CVE	Common Vulnerability and Exposures dictionary
CVSS	Common Vulnerability Scoring System
NVD	National Vulnerability Database
Regression Testing	Verify the installations required for testing do not have any issues with running system
Integration Testing	Test using two or more components together