**Chapter 15: Security Assessment and Testing**

Security tests verify that a control is functioning properly.

Security assessments are comprehensive reviews of the security of a system, application, or other tested environment.

Security audits use many of the same techniques followed during security assessments but must be performed by independent auditors.

There are three main types of audits: internal audits, external audits, and third-party audits.

Internal audits are performed by an organization’s internal audit staff and are typically intended for internal audiences.

External audits are performed by an outside auditing firm. These audits have a high degree of external validity because the auditors performing the assessment theoretically have no conflict of interest with the organization itself.

Third-party audits are conducted by, or on behalf of, another organization under a contract or law.

SOC Audit - A common standard used by auditors to perform assessments of service organizations. The intent is to allow the organization to conduct an external assessment instead of multiple third-party assessments and then share the resulting report with customers.

SOC 1 Engagements - Audit financial reporting

SOC 2 Engagements- Security Audit

SOC 3 Engagements- Security Audit when the results are intended for public disclosure

Type 1 Reports - Provide auditor’s opinion on the design of controls based on inputs (paper work) from the management. More of a documentation review. Valid for point in time.

Type 2 Reports - Provide auditor’s opinion on the operating effectiveness of the controls. The auditors not only check the paperwork; they also go and verify that the controls function properly. Valid for at least 6 months.

Network Discovery Scanning

TCP SYN Scanning  - Sends a single packet to each scanned port with the SYN flag set. If the scanner receives a response that has the SYN and ACK flags set, this indicates that the system is moving to the second phase in the three-way TCP handshake and that the port is open.

TCP Connect Scanning - Similar to SYN Scan but completes the three way handshake. This scan is usually done when users don't have sufficient privileges to craft raw requests.

TCP ACK Scanning  - Sends a packet with the ACK flag set, indicating that it is part of an open connection. This type of scan may be done in an attempt to determine the rules enforced by a firewall and the firewall methodology.

UDP Scanning - Performs a scan of the remote system using the UDP protocol, checking for active UDP services.

Xmas Scanning  Sends a packet with the FIN, PSH, and URG flags set. A packet with so many flags set is said to be “lit up like a Christmas tree,” leading to the scan’s name.

Fuzz testing is an important tool, but it does have limitations. Fuzz testing typically doesn’t result in full coverage of the code and is commonly limited to detecting simple vulnerabilities that do not require complex manipulation of business logic.

There are two main categories of fuzz testing:

Mutation (Dumb) Fuzzing  Takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input.

Generational (Intelligent) Fuzzing  Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program.

Interface testing assesses the performance of independent modules put together to ensure that they will work together properly when all the development efforts are complete.

Three types of interfaces should be tested during the software testing process:

* Application Programming Interfaces (APIs)
* User Interfaces (GUIs and CLIs)
* Physical Interfaces ( if applicable)

Misuse case testing identifies known ways that an attacker might exploit a system and tests explicitly to see if those attacks are possible in the proposed code.

Test coverage is highly subjective. Different criteria such as branch coverage, function coverage, condition coverage can be adopted for the analysis.

test coverage = number of use cases tested/ total number of use cases

Security Management processes are a critical feedback loop in the security assessment process because they provide management oversight and have a deterrent effect against the threat of insider attacks.

Account management reviews ensure that users only retain authorized permissions and that unauthorized modifications do not occur.

PCI DSS requires that organization scan the application at least annually and after any change in the application.