Software Security Assurance

Software Security Assurance

SSA Knowledgebase

Knowledgebase Search

Rows per page: 30 Search

Software Security Test Cases

Authentication Testing

Authorization Testing

Testing Audit Trails

Testing Audit Trails

1. Testing audit trail generation

Objective: To test if critical events are properly captured.

Test case ID	Description	Expected results
Audit.1.1	Validate if trails for all critical events (login, logout, transactions) are generated	Audit trail for all critical events are generated
Audit.1.2	Validate if sensitive information (i.e. credentials, Personally Identifiable Information (PII), credit card details) are not logged	Sensitive information is not logged
Audit.1.3	Validate if audit trail include, time of event, source of event, user account used for influencing event, event data and components impacted by event	Trail satisfies all requirements
Audit.1.4	Validate if frequency for trail generation is defined (i.e. every occurrence of event, once in x minutes,	For each event periodicity is defined

Test case ID	Description	Expected results
	every instance after y instances)	

2. Testing audit trail storage

Objective: To test if audit trails are stored properly.

Test case ID	Description	Expected results
Audit.2.1	Validate if trail limited by storage size	Trails are not limited by storage size. New file is generated once storage limit is reached
Audit.2.2	Validated if old events are removed once storage limit is reached	Old events are not removed. New file is generated for storage
Audit.2.3	Validate if audit trails are backed up at periodic interval	Trail are backed up at periodic interval
Audit.2.4	Validate if compression of file happens without altering the meaning of its content	Compression do not change file content
Audit.2.5	Check if log reduction (removing unnecessary events or data) do not remove audit trails for sensitive events	Log reduction is not happening
Audit.2.6	Check if log conversion is changing original data	Log conversion changes format however data remains intact
Audit.2.7	Validate if log normalization (converting multiple logs into same time zone for analysis) process is correct	NTP (Network time protocol) is used and all system components are generating logs in same time zone so no need to normalization
Audit.2.8	Check Hash (SHA) for each archived audit trail file to ensure its integrity	Write once media is used to store archive d files and Hash for each file is maintained
Audit.2.9	Check if unwanted event or data can be dispose without impacting other events	It is possible to dispose unwanted events along with its data. Only Admin has permission for it and such events are also logged.
Audit.2.10	Check how audit trail preservation requirements from legal/regulatory perspective are managed	Audit trails required for legal/regulatory compliance are generated separately from trouble shooting trails. All compliance trails are labeled and stored as per compliance requirement and protected with access control.

3. Testing event information transmission

Objective: To test if audit trail event information can be altered in transit or event source can be tampered

Test case ID	Description	Expected results
Audit.3.1	Check if events are accepted from authorised sources	Events from authorised sources are accepted and events generated from unauthorised sources are sent as an alert to administrators
Audit.3.2	Validate if there is clarity on which events shall be stored locally and centrally	All events are stored centrally
Audit.3.3	Validate if event data can be sniffed	Event data can't be sniffed as communication between source and destination happens over SSL/TLS
Audit.3.4	Validate if compression of file happens without altering the meaning of its content	Compression do not change file content
Audit.3.5	Check if data alteration can be detected	For each event Hash (SHA) is generated so data alterations are detected and alert is generated for administrators when such occurrences are detected
Audit.3.6	Check frequency of event information transmission	Audit event information transmission happens on event occurrence

4. Testing time synchronization amongst multiple components of audit trail

Objective: To test if audit trail time stamps in multi-component system are synchronised

Test case ID	Description	Expected results
Audit.4.1	Validate all the systems are in same time zone	All systems are in same time zone and time is synchronised with NTP

5. Testing traceability for critical events

Objective: To test if any of critical event can be traced to reconstruct sequence

Test case ID	Description	Expected results
Audit.5.1	Check if event sequence can be tracked through audit logs of multiple components	Event sequence can be constructed using logs from multiple components
Audit.5.2	Validate if event correlation (finding relation between one or more audit entries) possible with trail categories.	Event correlation is possible with event source, account, time stamp and event type

6. Testing log parsing & filtering

Objective: To test if logs can be parsed and filtered for analysis

Test case ID	Description	Expected results
Audit.6.1	Check if log formats can be parsed and filtered based on event information	Logs can be parsed and filtered based on event source, account, time stamp and event type
Audit.6.2	Validate if logs can be displayed in human readable format	Logs are displayed in Human readable format

7. Testing audit trail access permissions

Objective: To test if audit trails can be accessed by unauthorized sources

Test case ID	Description	Expected results
Audit.7.1	Validate if audit trail access permissions are set for authorized users only	Audit trails are accessed only by authorized users
Audit.7.2	Validate if administrative activity audit trails are generated separately and access is provided separately	Administrative activity audit trails are maintained separately
Audit.7.3	Audit trail clearance (removing entries based on time stamp) is allowed only to authorised users	Audit trail clearance is done by administrators and is tracked with separate administrator's audit trail

Testing Session Management

Data Security Testing

Testing for Client Side Attacks

Testing Data Validation

Buffer Overflow Testing

Configuration Testing