STAR

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Report ID		**Date**	
Lead Auditor		**Test Date Duration**	
Scope and Index		**Vectors**	
Channels		**Test Type**	

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE	**COMPANY STAMP/SEAL**

OPST Certification #		**OPSA Certification #**	

OPERATIONAL SECURITY VALUES

Visibility	
Access	
Trust	

LIMITATIONS VALUES

Vulnerability	
Weakness	
Concern	
Exposure	
Anomaly	

CONTROLS VALUES

Authentication	
Indemnification	
Resilience	
Subjugation	
Continuity	
Non-Repudiation	
Confidentiality	
Privacy	
Integrity	
Alarm	

OpSec		**True Controls**	
Limitations		**Security Δ**	

True Protection		**Actual Security**	

OVERVIEW

This Open Source Security Testing Methodology Manual provides a methodology for a thorough security test. A security test is an accurate measurement of security at an operational level, void of assumptions and anecdotal evidence. A proper methodology makes for a valid security measurement that is consistent and repeatable.

ABOUT ISECOM

ISECOM, the creator and maintainer of the OSSTMM, is an independent, non-profit security research organization and certification authority defined by the principles of open collaboration and transparency.

RELATED TERMS AND DEFINITIONS

This report may refer to words and terms that may be construed with other intents or meanings. This is especially true within international translations. This report attempts to use standard terms and definitions as found in the OSSTMM 3 vocabulary, which has been based on NCSC-TG-004 (Teal Green Book) from the US Department of Defense where applicable.

PURPOSE

The primary purpose of this Audit Report is to provide a standard reporting scheme based on a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. The secondary purpose is to provide guidelines which when followed will allow the auditor to provide a certified OSSTMM audit.

PROCESS

This Audit Report must accompany the full security test report document that provides evidence of the test and the results as defined in the statement of work between the testing organization and the client.

VALIDITY

For this OSSTMM Audit Report to be valid, it must be filled out clearly, properly, and completely. The OSSTMM Audit Report must be signed by the lead or responsible tester or analyst and accompany include the stamp of the company which holds the contract or sub-contract of the test. This audit report must show under COMPLETION STATUS which Channel and the associated Modules and Tasks have been tested to completion, not tested to completion, and which tests were not applicable and why. A report which documents that only specific parts of the Channel test have been completed due to time constraints, project problems, or customer refusal may still be recognized as an official OSSTMM audit if accompanied by this report clearly showing the deficiencies and the reasons for those deficiencies.

CERTIFICATION

OSSTMM certification is the assurance of an organization's security according to the thorough tests within the OSSTMM standard and is available per vector and channel for organizations or parts of organizations that maintain a rav level of a minimum of 90% validated yearly from an independent third-party auditor. Validation of security tests or quarterly metrics is subject to the ISECOM validation requirements to assure consistency and integrity.

1. POSTURE REVIEW

	TASK	COMMENTS	COMPLETION STATUS
1.1	Identified business objectives and markets.		
1.2	Identified legislation and regulations applicable to the targets in the scope.		
1.3	Identified business policies.		
1.4	Identified business and industry ethics policies.		
1.5	Identified operation cultures and norms.		
1.6	Identified operation times and flows applicable to the targets in the scope.		
1.7	Identified all necessary Channels for this scope.		
1.8	Identified all Vectors for this scope.		

2. LOGISTICS

	TASK	COMMENTS	COMPLETION STATUS
2.1	Applied testing safety measures.		
2.2	Determined and accounted for test instabilities.		
2.3	Determined and accounted for downtime in scope.		
2.4	Determined and accounted for test pace according to the test environment and the security presence.		

3. ACTIVE DETECTION VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
3.1	Determined and accounted for interferences.		
3.2	Tested with both interferences active and inactive.		
3.3	Determined restrictions imposed on tests.		
3.4	Verified detection rules and predictability.		

4. VISIBILITY AUDIT

	TASK	COMMENTS	COMPLETION STATUS
4.1	Determined targets through all enumeration tasks.		
4.2	Determined new targets by researching known targets.		

5. ACCESS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
5.1	Verified interactions with access points to all targets in the scope.		
5.2	Determined type of interaction for all access points.		
5.3	Determined source of interaction defined as a service or process.		
5.4	Verified depth of access.		
5.5	Verified known security limitations of discovered access points.		
5.6	Searched for novel circumvention techniques and security limitations of discovered access points.		

6. TRUST VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
6.1	Determined interactions that rely on other interactions to complete the test interaction according to the tasks.		
6.2	Determined targets with trust relationships to other targets in the scope to complete interactions.		
6.3	Determined targets with trust relationships to other targets outside the scope to complete interactions.		
6.4	Verified known security limitations of discovered trusts between the trusts.		
6.5	Verified known security limitations of discovered trusts between targets in the scope and the trusted interactions.		
6.6	Searched for novel circumvention techniques and security limitations of discovered trusts.		

7. CONTROLS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
7.1	Verified controls for Non-Repudiation functioning according to all tasks.		
7.2	Verified controls for Confidentiality functioning according to all tasks.		
7.3	Verified controls for Privacy functioning according to all tasks.		
7.4	Verified controls for Integrity functioning according to all tasks.		
7.5	Verified controls for Alarm functioning according to all tasks.		
7.6	Verified known security limitations of all controls Class B categories.		
7.7	Searched for novel circumvention techniques and security limitations of all controls Class B categories.		

8. PROCESS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
8.1	Determined all processes controlling the action of interactivity with each access.		
8.2	Verified the interaction operates within the confines of the determined process.		
8.3	Verified the interaction operates within the confines of the security policy for such interactions.		
8.4	Determined the gap between the operations of interactions and the requirements of posture from the Posture Review.		
8.5	Verified known security limitations of discovered processes.		
8.6	Searched for novel circumvention techniques and security limitations of discovered processes.		

9. CONFIGURATION AND TRAINING VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
9.1	Verified configuration/training requirements according to the posture in the Posture Review.		
9.2	Verified the application of appropriate security mechanisms as defined in the Posture Review.		
9.3	Verified the functionality and security limitations within the configurations/training for the targets in the scope.		
9.4	Searched for novel circumvention techniques and security limitations within configurations/training.		

10. PROPERTY VALIDATION

	TASK	COMMENTS	COMPLETION STATUS
10.1	Determined the amount and type of unlicensed intellectual property distributed within the scope.		
10.2	Verify the amount and type of unlicensed intellectual property available for sale/trade with the seller originating within the scope.		

11. SEGREGATION REVIEW

	TASK	COMMENTS	COMPLETION STATUS
11.1	Determined the amount and location of private information as defined in the Posture Review available through the targets.		
11.2	Determined the type of private information as defined in the Posture Review available within the scope.		
11.3	Verified the relationship between publicly accessible information outside the target detailing private or confidential information defined in the Posture Review and the scope.		
11.4	Verified the accessibility of public accesses within the target to people with disabilities.		

12. EXPOSURE VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
12.1	Searched for available targets through publicly available sources outside of the scope.		
12.2	Searched for available organizational assets as defined in the Posture Review through publicly available sources outside of the scope.		
12.3	Determined access, visibility, trust, and controls information available publicly within the targets.		
12.4	Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information within the targets.		
12.5	Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information outside the scope.		

13. COMPETITIVE INTELLIGENCE SCOUTING

	TASK	COMMENTS	COMPLETION STATUS
13.1	Determined the business environment of partners, suppliers, workers, and market through publicly available information on targets within the scope.		
13.2	Determined the business environment of partners, vendors, distributors, suppliers, workers, and market through publicly available information outside the scope.		
13.3	Determined the organizational environment through publicly available information on targets within the scope.		
13.4	Determined the organizational environment through publicly available information outside the scope.		

14. QUARANTINE VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
14.1	Verified quarantine methods for interactions to the targets in the scope.		
14.2	Verified quarantine methods for interactions from the targets to other targets outside the scope.		
14.3	Verified length of time of quarantine.		
14.4	Verified quarantine process from receive to release.		
14.5	Verified known security limitations of discovered quarantines.		
14.6	Searched for novel circumvention techniques and security limitations of discovered quarantines.		

15. PRIVILEGES AUDIT

	TASK	COMMENTS	COMPLETION STATUS
15.1	Verified the means of legitimately obtaining privileges for all authenticated interactions.		
15.2	Verified the use of fraudulent identification to obtain privileges.		
15.3	Verified the means of circumventing authentication requirements.		
15.4	Verified the means of taking non-public authentication privileges.		
15.5	Verified the means hijacking other authentication privileges.		
15.6	Verified known security limitations of discovered authentication mechanisms to escalate privileges.		
15.7	Searched for novel circumvention techniques and security limitations of discovered authentication mechanisms to escalate privileges.		
15.8	Determined depth of all discovered authentication privileges.		
15.9	Determined re-usability of all discovered authentication privileges on the authentication mechanisms on all targets.		
15.10	Verified requirements towards obtaining authentication privileges for discriminatory practices according to the Posture Review.		
15.11	Verified means towards obtaining authentication privileges for discriminatory practices for people with disabilities.		

16. SURVIVABILITY VALIDATION AND SERVICE CONTINUITY

	TASK	COMMENTS	COMPLETION STATUS
16.1	Determined measures applicable to disrupt or stop service continuity to and from the targets.		
16.2	Verified continuity processes and safety mechanisms active for the targets.		
16.3	Verified known security limitations of discovered safety and service continuity processes and mechanisms.		
16.4	Searched for novel circumvention techniques and security limitations of discovered safety and service continuity processes and mechanisms.		

17. END SURVEY, ALERT AND LOG REVIEW

	TASK	COMMENTS	COMPLETION STATUS
17.1	Verified methods for recording and alerting interactions to the targets in the scope.		
17.2	Verified methods for recording and alerting interactions from the targets to other targets outside the scope.		
17.3	Verified speed of recording and alerting.		
17.4	Verified persistence of recording and alerting.		
17.5	Verified integrity of recording and alerting.		
17.6	Verified distribution process of recording and alerting.		
17.7	Verified known security limitations of discovered recording and alerting methods.		
17.8	Searched for novel circumvention techniques and security limitations of discovered recording and alerting methods.		