National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Tenable Network Security, Inc. Tenable Security Center 3.2 and Components

Report Number: CCEVS-VR-VID10273-2010

Dated: 29 January 2010

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Deborah Downs (Senior Validator)

Aerospace Corporation

El Segundo, California

Mike Allen (Lead Validator)

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation (SAIC), Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated. Prospective users should read the Validator Comments in Section 10 carefully.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Tenable Security Center 3.2, the target of evaluation (TOE), conducted by the Science Applications International Corporation (SAIC), Incorporated, the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation by SAIC was performed in accordance with the United States Common Criteria Evaluation and Validation Scheme and was completed in January, 2010. The information in this report is largely derived from the ST, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by a separate group at SAIC (not part of the evaluation team) for Tenable Network Security, Incorporated. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.3 and AVA_MSU.1 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005. The TOE is conformant to the Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP).

The TOE is a suite of software products that provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, data leakage detection, event management and configuration auditing.

Tenable Security Center 3.2 consists of five main components:

- The Tenable Security Center 3.2 (SC3).
- 3D Tool 1.2 (3DT).
- Log Correlation Engine 2.0.2 (LCE).
- Passive Vulnerability Scanner 3.0 (PVS).
- Nessus Scanner 3.0.4 (Nessus).

Support for other intrusion detection system (IDS) products (e.g., scanners) is provided by the product but is not part of the evaluated configuration (i.e., their security functions were not evaluated).

The TOE provides administrators with tools to facilitate network security by providing the following services:

- Vulnerability discovery and management,
- Security event management and incident response,
- Measuring and demonstrating configuration management, and
- Dynamic and static asset discovery.

The TOE provides an integrated environment for managing security events and vulnerabilities. The Nessus, PVS, and LCE TOE components contain plug-ins (or scripts) that provide functionality specific to the TOE component. The TOE facilitates the administration and organization of security workflow and management tasks, including automatic reporting to affected parties; division of duties; access control for application data; and update and tracking of vulnerability closure.

Information gathered by the TOE for the above tasks is stored in a centralized database. The reporting, ticketing, user interface and security model are designed to ensure that the right people in the organization can access the information they need to make informed network security and performance decisions.

1.1. Interpretations

The Evaluation Team performed an analysis of the international and NIAP interpretations of the CC and the CEM and determined that no international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List (http://www.niap-ccevs.org/vpl/).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Tenable Security Center 3.2 and Components.
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP)
Security Target	*Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Security Target,* Version 1.0, dated January 15, 2010.
Dates of evaluation	March 2007 through January 2010
Evaluation Technical Report	*Final Evaluation Technical Report for Tenable Network Security, Inc. Tenable Security Center 3.2 and Components (Part I) Version 1.2*, Dated January 15, 2010 (Non-proprietary). *Final Evaluation Technical Report for Tenable Network Security, Inc. Tenable Security Center 3.2 and Components (Part II) Version 1.2*, Dated January 15, 2010 (Proprietary).
Conformance Result	Part 2 extended and Part 3 conformant, EAL 2 augmented with ALC_FLR.3 and AVA_MSU.1, and the IDSSPP
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007

Sponsor	Tenable Network Security, Inc., 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046
Developer	Tenable Network Security, Inc., 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046
Evaluators	James Arnold, Craig Floyd and Jean Petty of SAIC Incorporated
Validation Team	Deborah Downs and Mike Allen of The Aerospace Corporation

3. SECURITY POLICY

The following are the security policies enforced by the TOE.

3.1. Security Audit

The TOE generates audit events for the basic level of audit. (Note that the IDS_SDC.1 (EXP) and IDS_ANL.1 (EXP) requirements address a different audit mechanism that records the results from IDS scanning, sensing, and analyzing tasks. This is not that mechanism.) The TOE provides an SC3 GUI that is used by authorized system administrators to read the audit trail, and to sort audit data. The TOE audit events can be included in or excluded from reports based on event type. The TOE restricts access to the audit trail to authorized system administrators. The events that are audited are fixed and no event can be masked so that it is not entered into the audit trail.

The TOE administrator guidance advises the systems administrator how to configure and manage the TOE security audit storage so that storage exhaustion is prevented. If audit trail storage becomes exhausted, the TOE will overwrite the oldest record and send an alarm.

3.2. Identification and Authentication

TOE users are required to login with a unique name and password in order to access the TOE. Only systems administrators have access to security management functions. The TOE maintains user identities, authentication data, authorization information and role association. The SC3 provides a web-based logon and users must be successfully identified and authenticated prior to accessing the reports.

3.3. Security Management

The Security Center restricts the ability to manage functions based on the user role. The roles supported by the Security Center are Security Center Administrator (SCA), Primary Security Manager (PSM), Security Manager (SM) and End User (EU), (which collectively conform to the IDSSYPP Authorized Systems Administrator role). A Systems Administrator (which conforms to the IDSSYPP Authorized Administrator role) manages the environment. It is up to the TOE user organization to appropriately assign people to roles.

3.4. Protection of the TSF

The TOE protects itself and ensures that its policies are enforced in a number of ways. While there is dependence on the underlying operating system to separate its process constructs, enforce file access restrictions, and to provide communication services, the TOE protects itself by keeping its context separate from that of its users and also by making use of the operating system mechanisms to ensure that memory and files used by the TOE have the appropriate access settings. Furthermore, the TOE interacts with users through well-defined interfaces designed to ensure that its security policies are always enforced.

3.5. Intrusion Detection System

The TOE collects network traffic data for use in scanning, sensing and analyzing functions with the SC3. The TOE performs signature analysis on collected network traffic data and records corresponding network traffic event data. Reports are generated using a web-based interface to LCE that provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion. Note that users can only access reports via a web browser where access to TOE data is based on identification and authentication. The TOE provides the ability to generate alarms and notify a systems administrator using a configured notification mechanism when an intrusion is detected.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

Note that these are drawn from the IDSSPP with the exception of A.WKSTN and A.OS whereby it is assume that workstations associated with the TOE will be secured and servers hosting the TOE will be dedicated to that purpose.

4.1. Physical Security Assumptions

The following physical assumptions are identified in the Security Target.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.2. Personnel Security Assumptions

The following personnel assumptions are identified in the Security Target.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and its environment and the security of the information it contains.

A.NOEVIL The authorized administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation and that of its environment.

A.NOTRST The TOE can only be accessed by authorized users.

4.3. Operational Security Assumptions

The following are the operational use assumptions identified in the Security Target.

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.WKSTN All desktop systems used to access security center data (either through the web GUI or through 3D Tool) must be secured, patched and have the latest anti-virus software installed.

A.OS The operating system for each component, Security Center, Nessus, LCE, and PVS, must be dedicated to the associated application and configured in a secure manner to ensure the security controls cannot be bypassed.

4.4. Organizational Security Policies

The following are the organizational policies addressed by the product. Note that these are all drawn from the IDSSPP.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4.5. Clarification of Scope

The following functionality of the SC3 components is not included in the evaluation and should not be used by customers desiring the evaluated configuration:

- The use of other intrusion detection system products (e.g., scanners) and the SC3 interface to support other scanners.
- The interfaces of the Nessus, PVS, and LCE components intended for use of the component independent of the other components.
- The use of third party authentication (e.g., LDAP, Radius, TACACS, etc.)
- The use of the PVS capability to take actions to mitigate IDS-related events.
- The LCE clients that operate within non-TOE components have not been subject to the evaluation. *However, while their impact on their respective hosts is uncertain,*

they cannot impact the security claims in this ST and as such are not forbidden in the evaluated configuration.

- Nessus scans that are deemed potentially harmful are not supported in the evaluated configuration.

- Exporting data (from any TOE component) via SYSLOG outside the TOE is not allowed in the evaluated configuration

5. ARCHITECTURAL INFORMATION

The Target of Evaluation (TOE) is Tenable Security Center 3.2 (SC3) and Components: 3D Tool 1.2 (3DT); Log Correlation Engine 2.0.2 (LCE); Passive Vulnerability Scanner 3.0 (PVS); and, Nessus Scanner 3.0.4 (Nessus). The TOE consists of only these five Tenable products, as shown in the Figure 1. The configuration of the TOE subject to evaluation consists of a single SC3 and at least one instance each of the Nessus, PVS, LCE, and 3DT products. Support for other intrusion detection system (IDS) products (e.g., scanners) is provided by the product but is not part of the evaluated configuration (i.e., their security functions were not evaluated).

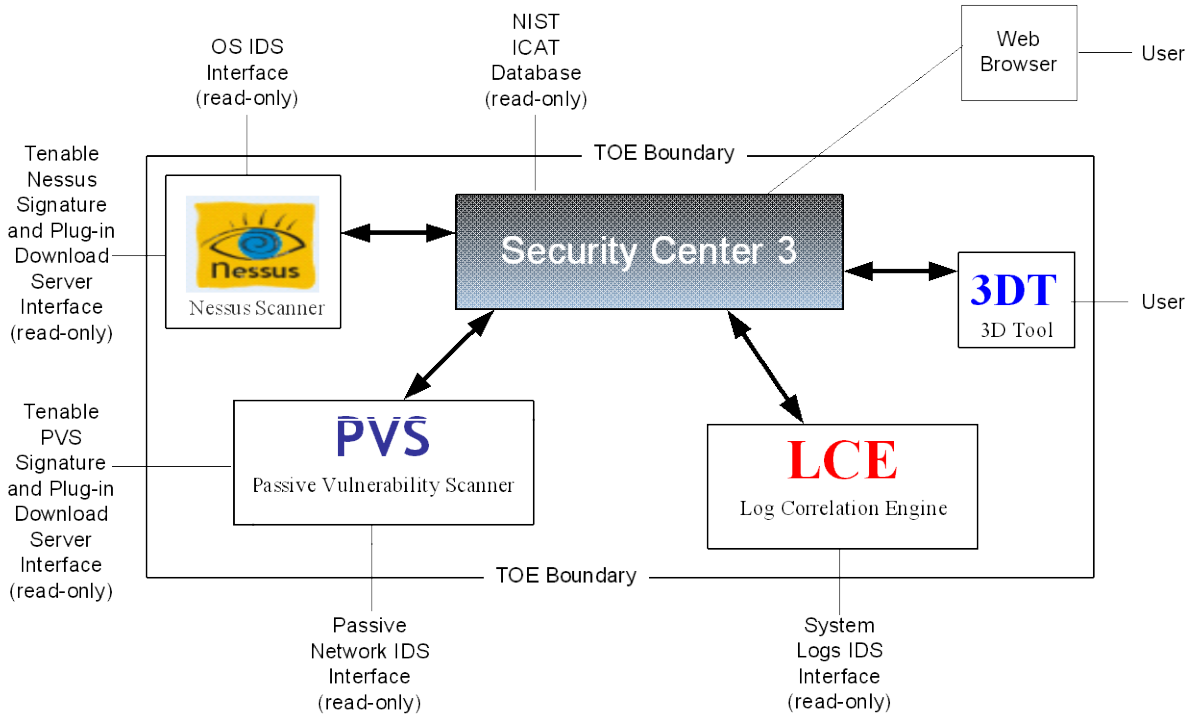

Figure 1 – The Tenable products comprising the TOE.

Figure 1 shows the external interfaces to the TOE. The TOE initiates all except the user interfaces.

5.1. Security Center

The Security Center application is the management module that ties all of the other components together and enables enterprise wide vulnerability, event and log management, analysis, and reporting. All security management happens through the Security manager where policies are maintained and data collected for controlled access by administrators and other TOE users.

5.2. Nessus Vulnerability Scanner

The Nessus Vulnerability Scanner is an active scanner that provides agent-less host auditing of both UNIX and Windows servers. It features network node discovery, asset profiling, and vulnerability analysis. Nessus scanners can be distributed throughout a large network, on DMZs, and across distributed networks. It can be used for ad-hoc scanning, daily scans, and quick-response audits. While Nessus could potentially be used as a stand-alone product, once it is configured into the TOE and is associated with a Security Center it is managed through the Security Center and provides results back to the Security Center which is its only client.

5.3. Log Correlation Engine

The Log Correlation Engine aggregates, normalizes, correlates and analyzes event log data from the various devices within the network infrastructure. It is closely integrated with the Security Center, allowing the centralization of log analysis and vulnerability management.

5.4. Passive Vulnerability Scanner

The Passive Vulnerability Scanner continuously monitors network traffic, searching for vulnerable systems, watching for potential application compromises, observing client and server trust relationships, and tracking open or browsed network protocols in use. The Passive Scanner maps new hosts and services as they appear on the network and monitors for vulnerabilities. Like the other components in the evaluated configuration, the Passive Vulnerability Scanner is configured to be managed by the Security Center and to return its results to the Security Center.

5.5. 3D Tool

The 3D Tool is a 3D Visualization tool that runs on a user workstation and displays network topology and the relative distribution of security information in three dimensions. Unlike the other components, the 3D Tool is an application program exercised by users. When invoked it uses the user's logon credentials to connect to the Security Center in order to access data to which the user is authorized and then to display that data in a variety of graphical displays which may be preferable to the user.

While each component can be configured on the same or different hosts, they have all been designed to utilize encryption capabilities of their hosts OSs to encrypt (using SSL or SSH depending on the components) any data that might be sent over a network connection. Furthermore, each component relies on its host for protection and except for the 3D Tool it is expected that the hosts are dedicated to the purposes of the TOE. Please refer to the Security Target for more technical details about the product and its associated security claims.

6. DOCUMENTATION

Following is a summary of user documents supplied by the developer for the TOE:

- Tenable Common Criteria Evaluated Configuration Guide [ECG], October 29, 2009 (Revision 4)
- Security Center 3.2 [SC3.2] Documentation (Revision 57)
- Security Center 3.2 Quick Start Guide (Revision 16)
- 3D Tool 1.2 User Guide (Revision 7)
- Nessus 3.2 Installation Guide (Revision 37)
- Nessus 3.2 Advanced User Guide (Revision 9)
- Nessus Credential Checks for Unix and Windows (Revision 17)
- Nessus Compliance Checks Auditing UNIX and Windows Device Configurations (Revision 27)
- NessusClient 3.2 User Guide (Revision 3)
- Log Correlation Engine 2.0 Administration and User Guide (Revision 25)
- Log Correlation Engine 2.0 Client Guide (Revision 18)
- Log Correlation Engine 2.0 Log Analysis Guide (Revision 7)
- Log Correlation Engine 2.0 Large Disk Array Install Guide (Revision 5)
- TASL Reference Guide (Revision 14)
- Log Correlation Engine 2.0 Statistics Daemon Guide (Revision 13)
- Passive Vulnerability Scanner 3.0 User Guide (Revision 11)

The security target used is:

- Tenable Network Security, Inc. Tenable Security Center 3.2 and Components, Security Target Version 1.0, 15 January 2010

7. IT PRODUCT TESTING

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL2+ evaluation.

7.1. Developer testing

The developer selected a small subset of their overall tests in order to fulfill the test requirements for an EAL2+ evaluation. The selection was chosen to provide representative testing of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan and a series of IDS-related supplemental test procedures where the results of the tests are presented as actual screen shots and prose summaries.

7.2. Evaluator Independent Testing

Independent testing took place in essentially two phases.

During the initial phase, the evaluator exercised the developers test plan (without the IDS-related supplemental test procedures). This involved installing and configuring the Security Center on a Red Hat Linux Enterprise Server 4 server host; the LCE on a Red Hat Linux Enterprise Server 4 server host; and PVS, Nessus, and LCE clients (for host monitoring) on each of Red Hat Linux Enterprise Server 4, Red Hat Linux Enterprise Server 3, and Windows 2003 SP2. The 3D Tool product was also installed on a Windows XP SP3 host. Subsequently, each (and every) test case in the test plan was exercised as instructed and the evaluators obtained the same results as were provided by the developer in their test results.

While the initial testing above touched on each of the security requirements in some way, those tests did not provide adequate depth with regard to demonstrating that the product could provide the full range of claimed intrusion and vulnerability scanning capabilities. The IDS-related supplemental test procedures were designed to provide insight into the depth of those capabilities. These tests were developed and documented through a collaborative effort between the evaluators and product developers to yield a set of test procedures and results. For the most part these tests were exercised by the developer with interaction, guidance and oversight by the evaluators.

7.3. Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. In addition, the evaluator revisited the following vulnerability sites to confirm the vendor's vulnerability assessment:

- http://cve.mitre.org
- http://osvdb.org
- http://secunia.com

The vendor's analysis was confirmed. Then the evaluator conducted scans of the test systems using the Nessus tool and confirmed that no vulnerabilities exist.

7.4. Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8. EVALUATED CONFIGURATION

The Target of Evaluation (TOE) is the Tenable Security Center 3.2 and Components. It consists of the Tenable Security Center 3.2 (SC3); 3D Tool 1.2 (3DT); Log Correlation Engine 2.0.2 (LCE); Passive Vulnerability Scanner 3.0 (PVS); Nessus Scanner 3.0.4 (Nessus). The TOE consists of five (5) distinct products and the evaluated configuration includes all of the Tenable products working together. The configuration of the TOE subject to evaluation consists of a single SC3 and at least one instance each of the Nessus, PVS, LCE, and 3DT component products.

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

SAIC has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.3 and AVA_MSU.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation and conducted several Validation Oversight Review boards. The evaluation effort was finished in January, 2010. A final Validation Oversight Review (VOR) was held on January 8, 2010 and final changes to the ST and ETR were completed on January 15, 2010.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the Tenable Network Security, Incorporated Tenable Security Center 3.2 and Components meet the claims stated in the Security Target. The validation team also wishes to add the following caveats to the use of the product and the evaluated configuration.

To be used in the evaluated configuration the users of the TOE must **not** make use of the following options and features:

- Other intrusion detection system products (e.g., scanners) and the SC3 interface to support other scanners.
- Interfaces of the Nessus, PVS, and LCE components intended for use of the component independent of the other components.
- Third party authentication servers (e.g., LDAP, Radius, TACACS, etc.)
- The PVS capability to take actions to mitigate IDS-related events.
- LCE clients that operate within non-TOE components
- Nessus scans that are deemed potentially harmful are not supported in the evaluated configuration.
- Exporting data (from any TOE component) via SYSLOG outside the TOE

In addition, it must be emphasized that the Tenable components must operate on one or more dedicated machines with no other applications present.

NOTE: It is important for users of the evaluated configuration to obtain the following supplement to the Tenable User's Guide to ensure proper configuration of the product:

- Tenable Common Criteria Evaluated Configuration Guide [ECG], October 29, 2009 (Revision 4)

11. ANNEXES

None

12. SECURITY TARGET

Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Security Target, Version 1.0, dated January 15, 2010.

13. GLOSSARY

- **Acronym List:**

3DT	3D Tool
CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CLI	Command Line Interface
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
EU	End User (a TOE role)
EXP	Explicitly stated SFR
FQDN	Fully Qualified Domain Name
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
HTTP	Hyper-text Transfer Protocol
ID	Identity/Identification
IDS	Intrusion Detection System
IDSSYPP	IDS System PP, Version 1.6, April 4, 2006.
IP	Internet Protocol
IT	Information Technology
ITT	Internal TOE TSF Data Transfer family of FPT
LCE	Log Correlation Engine
NASL	Nessus Attack Scripting Language
NIAP	National Information Assurance Partnership
NIDS	Network IDS
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PSM	Primary Security Manager (a TOE role)
PVS	Passive Vulnerability Scanner 2.2
SA	System Administrator (a TOE environment role)
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement

SC3	Security Center 3.0
SCA	Security Center Administrator (a TOE role)
SFR	Security Functional Requirement
SM	Security Manager (a TOE role)
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TASL	Tenable Application Scripting Language
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
US	United States
XML	Extensible Markup Language

14. BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005, ISO/IEC 15408-2.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, ISO/IEC 15408-2.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.0, July 2005, Revision 2.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, September 2006, Revision 1.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006

[9] Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Security Target, Version 1.0, January 15, 2010

[10] Final Evaluation Technical Report For Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Part I, Version 1.2, January 15, 2010

[11] Final Evaluation Technical Report For Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Part II (Proprietary), Version 1.2, January 15, 2010

[12] Evaluation Team Test Plan For Tenable Network Security, Inc. Tenable Security Center 3.2 and Components ETR Part 2 Supplement (SAIC and Tenable Proprietary), Version 2.0, March 21, 2008