National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Tenable SecurityCenter 4 and Components

Report Number: CCEVS-VR-VID10443-2012
Dated: 1 October 2012
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Aerospace Corporation
Columbia, Maryland

Bradford O'Neill (Senior Validator)
MITRE Corporation
Bedford, Massachusetts

Olin Sibert (Senior Validator)
Orion Security

Common Criteria Testing Laboratory

Anthony J. Apted
Julie A. Cowan
James Arnold
Quang Trinh
Science Applications International Corporation
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 that end-user in 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 and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Tenable SecurityCenter 4 and Components. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Tenable SecurityCenter 4 and Components was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in September 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Tenable Network Security, Inc. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R3, dated July 2009. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Tenable SecurityCenter 4 and Components Security Target. The Product is conformant to the Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a collection of software components as follows:

- SecurityCenter 4.4 (SC4);
- 3D Tool 2.0.1 (3DT);
- Log Correlation Engine 3.6.1 (LCE);
- Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows (PVS);

- Nessus scanner 5.0.1 (Nessus); and
- xTool 2.1.

The TOE components are configured as an intrusion and vulnerability detection system. The SC4 component collects vulnerability data from one or more instances of PVS sensors and one or more instances of Nessus scanners. It analyzes the data and presents the results to its users, with the help of one or more instances of LCE and 3DT components. The xTool has the ability to produce audit files for use by SC4 via Nessus scanning. This fits the IDS System structure specified in the IDSSYPP, to which this TOE claims conformance, as follows:

- IDS Analyzer: SC4 with LCE and 3DT.
- IDS Scanner: Nessus.
- IDS Sensor: PVS.

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
- Dynamic and static asset discovery

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The validation team monitored the activities of the evaluation team at discrete points during the evaluation, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2) have been met.

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 information technology (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.

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;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals 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 SecurityCenter 4 and Components
Protection Profiles	Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007.
Security Target	*Tenable SecurityCenter 4 and Components Security Target*, Version 1.0, September 13, 2012
Dates of evaluation	November 2010 through September 2012
Evaluation Technical Report	*Evaluation Technical Report for Tenable SecurityCenter 4 and Components Part 1 (Non-Proprietary)*, Version 1.0, September 13, 2012, and *Evaluation Technical Report for Tenable SecurityCenter 4 and Components Part 2 (Proprietary)*, Version 1.0, September 13, 2012
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on November 1, 2010
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009and all applicable NIAP and International Interpretations effective on November 1, 2010
Sponsor	Tenable Network Security, Inc., 7063 Columbia Gateway Drive, Columbia, MD 21046
Developer	Tenable Network Security, Inc.
Common Criteria Testing Lab	SAIC Inc., Columbia, MD

Evaluators	James Arnold, Julie Cowen, Catherine Sykes, Quang Trinh, and Anthony Apted of SAIC, Inc.
Validation Team	Olin Sibert of Orion Security, Bradford O'Neill of MITRE Corporation and Mike Allen of the Aerospace Corporation

2.1 Applicable Interpretations

There were no applicable NIAP or International Interpretations when the evaluation started.

3 Security Policy

The security requirements enforced by the Tenable SecurityCenter 4 and Components were designed based on the following overarching security policies:

3.1 Security Audit

The TOE generates audit records for at least the basic level of audit, including the following events.

Start-up and shutdown the SC4 component. If the SC4 component is enabled, then auditing is turned on and cannot be turned off.

- Access to the system by TOE users
- Access to the TOE and system data by other system components
- Successful and unsuccessful attempts to read from the audit trail
- Successful and unsuccessful attempts to launch scans
- Modifications to the audit configuration
- Successful and unsuccessful attempts at user identification and authentication
- Modifications to the TSF configuration and data
- Modifications to the TOE users' role assignments
- Each audit record contains at least the following information: date and time of the event, event type, subject identity, and event success or failure.

3.2 Identification and Authentication

The SC4 TOE component provides an HTTPS-based GUI login interface. TOE users are required to login to the SC4 TOE component with a unique name and password before access to the TOE is granted. The TOE maintains user identities, authentication data, authorization information and role association information for each user. Users must be successfully identified and authenticated prior to accessing any reports.

The SecurityCenter Administrator can configure the TOE to lock a specific account after a configurable number of consecutive unsuccessful login attempts occur. It is up to users to contact a SecurityCenter Administrator to request that a locked account be unlocked.

When using the 3DT and xTool clients, users must still authenticate successfully to the SC4. The 3DT client is simply an application that makes visualization more pleasant for the administrator. The 3DT application will pass authentication credentials to the SC4 to perform authentication before any TOE information can be displayed to the end user. The xTool

application will pass authentication credentials to the SC4 to perform authentication before any scan result or repository query information can be displayed to the end user.

3.3 Security Management

The IDSSYPP defines two roles: Authorized Administrator and Authorized System Administrator. The Authorized Administrator role is a TOE environmental role and is realized by the Systems Administrator role in the TOE. The Authorized System Administrator role is realized by four roles in the TOE. Those roles are: SecurityCenter Administrator, Organization Head, Manager, and End User. The term "TOE users" will be used when referring to all four of the TOE roles, since only the four administrative roles are allowed access by the TOE. Otherwise, each role will be identified specifically. The TOE restricts the ability to manage functions related to audit and system data to SecurityCenter Administrators. They are able to query and add system and audit data; and query and modify all other TOE data. Scanning, sensing and analyzing tasks are restricted to Organization Heads, Managers and End Users, who can modify the behavior of system data collection, analysis and reaction. The environment supports the Authorized Administrator role. Authorized Administrators manage the operating systems, and install and configure the TOE.

Organization Heads, Managers and End Users operate the IDS system on specific parts of the network domain space called an Organization. An Organization is made up of one or more managers who perform actions for the Organization. The Managers are expected to work together for an Organization. Organization Heads and Managers administer an Organization network and are able to initiate Organization analyzer IDS audit functions, access IDS audit data and manage user accounts. Only Organization Heads are able to add new IDS sources. End Users administer a specific sub-network within an Organization network. Depending on the size of the Organization, some or all of these roles may be assigned to one individual.

The Organization Head is the first account created for a TOE Organization. If the Organization Head account is deleted, the Organization is also deleted, even if other Manager accounts are active at the time.

The TOE maintains a directory structure in the host file system to hold data for specific Organizations. Subdirectories can be created to further subdivide Organization data according to sub-networks. The SecurityCenter Administrator creates this structure in the course of configuring Organizations and gives access to the Organization's Organization Head, who may then create other Managers and End Users. Organization Heads and Managers can restrict the access that End Users have within the Organization structure and thus restrict them to operating the IDS on specific subsets of the Organization network.

The TOE offers access by Organization Heads, Managers and End Users via these directories, according to the scope of their authority. Organization Heads and Managers can access Organization directories. End Users can access only specific subdirectories within an

Organization directory. This access is determined by the TOE. When an Organization Head account is deleted, the corresponding Organization directory is also deleted.

User access is restricted by the role to which the user is assigned and the assets to which the user has been granted access. All SC4 functions are controlled by asset lists. Individual SecurityCenter users are assigned one or more asset lists. These lists can be either static or dynamic. Users who have the ability to scan can only scan hosts in their asset lists. Similarly, users can only see vulnerability, compliance, intrusion detection, and normalized logs for systems within their asset groups. The role indicates what functionality (i.e., which menu options) the TOE presents to each user. The assets are the machines for which the user can launch IDS scans and access IDS audit records.

The Authorized Administrator environmental role is implemented by the underlying operating system, where it is called System Administrator or Administrator or Root. It has full access to the underlying operating system and, by implication, the entire TOE.

3.4 Intrusion Detection System

The TOE collects and records network traffic data for use by the scanning, sensing and analyzing functions with the SC4. The following event types are collected:

- Identification and authentication
- Data accesses
- Service Requests
- Network Traffic
- Security Configuration Changes
- Data Introduction
- Detected Malicious Code
- Access Control Configuration
- Service Configuration
- Authentication Configuration
- Accountability Policy Configuration

For each event, the TOE records at least the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The SecurityCenter Administrator can specify the types of events that will be audited by configuring the various PVS and Nessus scanners deployed in the monitored system. The TOE comes with several pre-configured audit configuration files that were derived from NSA and other guidelines for the configuration of Unix and Windows systems.

The TOE performs analysis on all signature, statistical and integrity data. Signature analysis involves identifying deviations from normal patterns of behavior (e.g., it may use mean frequencies and measures of variability to identify abnormal usage). Statistical analysis involves identifying patterns of usage that correspond to known attacks or misuses of the system (e.g., patters of system settings and user activity can be compared against a database of known attacks). Integrity analysis involves comparing system settings or user activity at some point in time with that at another point in time to detect (possibly unauthorized) differences. When analysis identifies an anomaly, the TOE records an analytical result that contains at least the date and time of the result, type of result, identification of data source, location and description.

Reports are generated using a web-based interface to SC4 that provides access to the LCE, allowing users to examine analytical conclusions and the information used to reach those conclusions in an intuitive way.

4 Assumptions and Clarification of Scope

Note that these assumptions 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 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 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 Intended Use Assumptions

The following intended use assumptions are 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.

4.4 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

4.5 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

4.6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this

evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

The following features are exclusions, assumptions, or configuration restrictions in the TOE evaluated configuration:

- Assumption: The evaluated configuration requires at least one instance of each identified TOE component.
- Exclusion: Use of Nessus, PVS or LCE components directly rather than via the SC4 interfaces is excluded from the evaluated configuration.
- Exclusion: Use of third party authentication servers, such as LDAP, is not allowed in the evaluated configuration..
- Exclusion: Custom roles are unique to each individual Organization and thus are excluded from the evaluated configuration.
- Configuration restriction: Exporting data (from any TOE component) via SYSLOG outside the TOE is not allowed in the evaluated configuration.
- Exclusion: The LCE clients that operate within non-TOE components have not been subject to the evaluation.
- Exclusion: The PVS's inability to interfere with network traffic has not been subject to the evaluation.

5 Architectural Information

The Target of Evaluation (TOE) is Tenable SecurityCenter 4 (SC4) and Components: SecurityCenter 4.4, 3D Tool 2.0.1 (3DT), Log Correlation Engine 3.6.1 (LCE), Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows (PVS), Nessus scanner 5.0.1 (Nessus), and xTool 2.1.

The TOE consists of only these six Tenable products, as shown in the Figure 1. The configuration of the TOE subject to evaluation consists of a single SC4 and at least one instance each of the Nessus, PVS, LCE, 3DT and xTool 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).

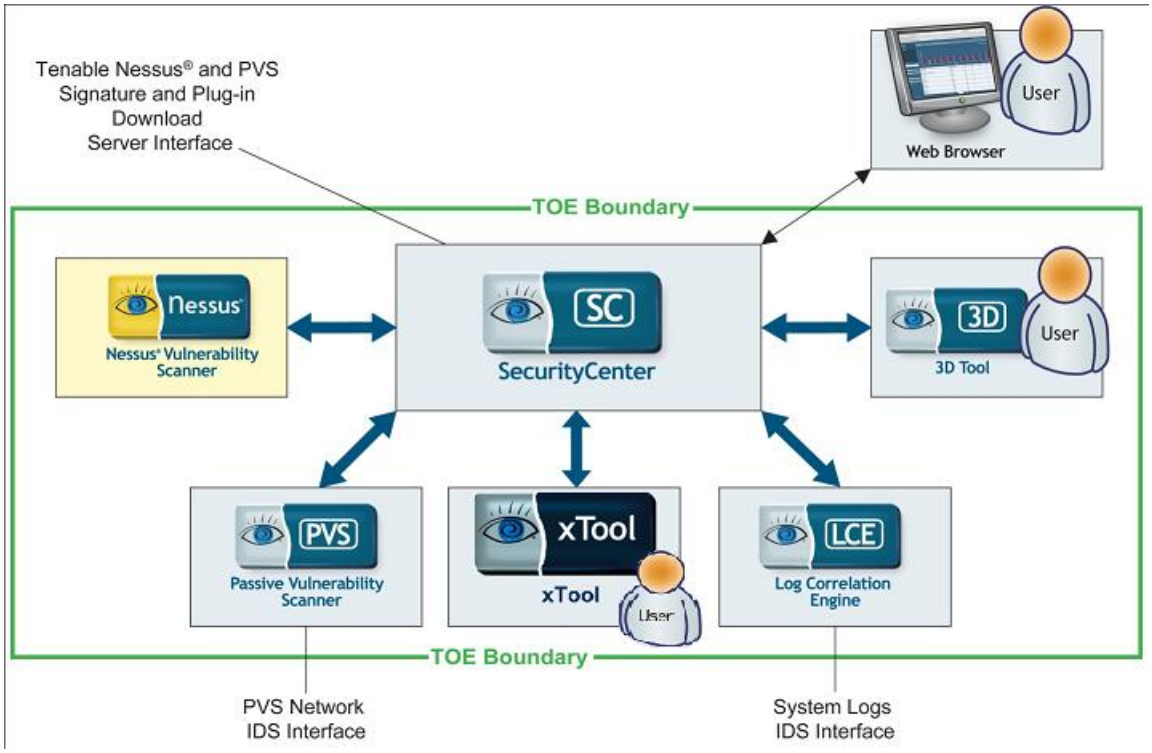

Figure 1 – The Tenable products comprising the TOE.

Figure 1 shows the external interfaces to the TOE. The TOE initiates all except the user interfaces. None are used to provide IDS information to external IT entities. The external interfaces are:

Passive Network IDS Interface – Interface to monitored networks to passively collect vulnerability information.

System Logs (SYSLOG Server) IDS Interface – Interface to monitored servers to collect IDS information. The interface uses the SYSLOG protocol to accept events from other components of the TOE.

Nessus Scanner Interface – Interface to monitored networks to actively collect vulnerability information.

Tenable Nessus Signature and Plugin Download Server – Interface to Tenable Nessus server to download signatures and NASL plugins that allow Nessus to detect the latest known attacks and vulnerabilities against operating systems. The downloaded signatures and plugins are configuration data that keep the product current with known vulnerabilities. They update the signatures and plugins that are shipped with the TOE.

Tenable PVS Signature and Plugin Download Server – Interface to Tenable PVS server to download signatures and PRM plugins that allow PVS to detect the latest known attacks and vulnerabilities from its network perspective. The downloaded signatures and plugins are configuration data that keep the product current with known vulnerabilities. They update the signatures and plugins that are shipped with the TOE.

3DT User Interface – User interface to SC4 using 3DT for an enhanced view of topology and vulnerability data.

xTool User Interface – User interface to xTool for conversion of XML data files to .audit file formats used by SC4.

Web Browser User Interface – User interface to SC4 using a standard web browser with an SSL connection.

Note that in theory, the Nessus can be used independently of SC. The other components, PVS and LCE, are also optional components to the SC. It is assumed that all components will be configured and managed by SC and any independent interfaces would not be used. Rather, SC4 would be used (sometimes via the 3DT component) to integrate and centralize those component capabilities.

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
- 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 plugins (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 databases used by SC and the LCE. 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.

The TOE consists of the six components shown above configured as an intrusion and vulnerability detection system. The SC4 component collects vulnerability data from one or more instances of PVS sensors and one or more instances of Nessus scanners. It analyzes the data and presents the results to its users, with the help of one or more instances of LCE and 3DT components. The xTool has the ability to produce audit files for use by SC4 via Nessus scanning. This fits the IDS System structure specified in the IDSSYPP, to which this ST claims conformance, as follows:

- IDS Analyzer: SC4 with LCE and 3DT.
- IDS Scanner: Nessus.
- IDS Sensor: PVS.

Although the xTool is part of the TOE as a standalone component that is used only to generate audit files from SCAP-validated content, the xTool does not interface directly with other TOE components. xTool audit files are generated for use by SecurityCenter, but the underlying operating system on which the xTool runs is responsible for the audit file upload function, and the xTool does not otherwise communicate or authenticate to the other TOE components.

xTool audit files are generated for use by SecurityCenter, but the underlying operating system on which the xTool runs is responsible for the audit file upload function. xTool is able to query repositories and scan results in SC4; to do so, it authenticates to SecurityCenter over SSL on TCP port 443 using valid SecurityCenter user credentials with permissions to perform such queries.

The SC4 component is able to interface with additional third-party generators of IDS event data, but that capability is not tested in this evaluation.

More information can be found in the Security Target.

6 Documentation

Following is a summary of the user guidance documents available with the TOE, which were evaluated as part of this evaluation:

Tenable Common Criteria Evaluated Configuration Guide, Revision 9, April 24, 2012

SecurityCenter 4.4 Administration Guide, Revision 1, April 17, 2012

3D Tool 2.0.1 User Guide, Revision 3, July 18, 2011

3D Tool 2.0.1 Quick Start Guide

xTool 2.1 User Guide, Revision 1, May 2, 2012

SecurityCenter 4.4 Architecture, Revision 1, April 17, 2012

SecurityCenter 4.4 Installation Guide, Revision 1, April 17, 2012

SecurityCenter 4.4 User Guide, Revision 1, April 17, 2012

Nessus 5.0 Installation and Configuration Guide, Revision 9, May 11, 2012

Nessus 5.0 User Guide, Revision 8, April 4, 2012

Nessus 5.0 XML-RPC Protocol Specification, Revision 1, June 11, 2012

Nessus Compliance Checks Auditing System Configurations and Content, Revision 60, March 22, 2012

Nessus Credential Checks for Unix and Windows, Revision 27, March 21, 2012

Passive Vulnerability Scanner 3.6 Linux User Guide, Revision 2, March 23, 2012

Passive Vulnerability Scanner 3.6 Windows User Guide, Revision 3, March 23, 2011

Log Correlation Engine 3.6 Administration and User Guide, Revision 7, May 7, 2012

Log Correlation Engine 3.6 Client Guide, Revision 8, May 7, 2012

Log Correlation Engine 3.6 Log Normalization Guide, Revision 3, May 31, 2011

Log Correlation Engine 3.6 Large Disk Array Install Guide, Revision 2, May 31, 2011

Log Correlation Engine 3.6 Statistics Daemon Guide, Revision 1, January 4, 2011

Log Correlation Engine 3.6 TASL Reference Guide, Revision 2, May 31, 2011

Tenable Product Delivery Process, Revision 3, January 27, 2011

The security target used is:

Tenable Network Security, Inc. Tenable SecurityCenter 4 and Components Security Target, Version 1.0, September 13, 2012

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 Tenable's 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 Independent Testing

The evaluators developed a test plan addressing TOE installation, use of developer-provided security functional tests, and independently created security functional and penetration tests. After testing the evaluators produced a test report describing the hand-on, independent testing effort.

The evaluators installed and configured each of the evaluated TOE components using the evaluated guidance documents. The SecurityCenter, PVS, LCE, and Nessus components were installed and configured (to interoperate) on Red Hat Enterprise Linux 5 hosts and instances of both the PVS and Nessus components were also installed on Microsoft Windows XP Professional hosts. All of the hosts were accessible using a Microsoft Windows-based laptop and remote desktop and SSH tools available from the host operating systems. That laptop hosted both the 3D Tool and xTool. Additionally, these hosts were configured with access to a network of target hosts with a range of issues (open ports, various component versions, etc.) for IDS scanning purposes. Lastly, Wireshark was installed on the SecurityCenter and also the test laptop so that applicable network session data could be collected.

The evaluators exercised all of the developer tests as well as their own tests finding the TOE to operate as claimed. The evaluators performed port scans on each of the component hosts in order to identify and rationale any open ports. The evaluators collected network sessions for the purpose of verifying that the connections between the SecurityCenter and all other components (except the xTool that doesn't communicate across the network) were encrypted as claimed. The evaluators also collected session traffic between the LCE and some LCE-clients in the environment to further ensure that network traffic was encrypted, though LCE clients are not included as TOE components in the evaluated configuration.

Ultimately, the tests exercised by the evaluators touched on every claimed security function as well as some security architecture aspects of the TOE. Given the breadth of tests directly and successfully exercised by the evaluators the testing requirements for EAL2+ are fulfill.

.

8 Evaluated Configuration

The Target of Evaluation (TOE) is Tenable SecurityCenter 4 (SC4) and Components: SecurityCenter 4.4, 3D Tool 2.0.1 (3DT), Log Correlation Engine 3.6.1 (LCE), Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows (PVS), Nessus scanner 5.0.1 (Nessus), and xTool 2.1. The TOE consists of six (6) 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 SC4 and at least one instance each of the Nessus, PVS, LCE, 3DT, and xTool component products.

9 Results of the Evaluation

The evaluation determined that the product meets the requirements for EAL 2 augmented with ALC_FLR.2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), Parts 1 and 2, which are controlled by SAIC Inc.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Tenable SecurityCenter 4 and Components meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The user of this product should carefully review the assumptions and restrictions on the evaluated configuration documented in the Clarification of Scope Section 4.6 of this report.

11 Security Target

Tenable Network Security, Inc. Tenable SecurityCenter 4 and Components Security Target, Version 1.0, September 13, 2012.

12 Glossary

The following abbreviations and definitions are used throughout this document:

3DT	3D Tool 2.0.1
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 3.6.1
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 3.6 for Linux/Unix and Windows
SA	System Administrator (a TOE environment role)
SAIC	Science Applications International Corporation

13 Bibliography

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

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009
- Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008
- Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007
- Tenable Network Security, Inc. Tenable SecurityCenter 4 and Components Security Target, Version 1.0, September 13, 2012
- Evaluation Team Test Report for Tenable SecurityCenter 4 and Components ETR Part 2 Supplement, Version 1.0, September 17, 2012

.