National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Retina Network Security Scanner Version 5.4.21.53

Report Number: CCEVS-VR-07-0044
Dated: 25 May 2007
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Ralph Broom
Noblis
Jerome F Myers
The Aerospace Corporation

Common Criteria Testing Laboratory

Tony Apted
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This document is intended to assist the end-user of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST) which is where specific security claims are made, and this Validation Report (VR) which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Retina Network Security Scanner Version 5.4.21.53. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation 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 May 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is **Common Criteria Part 2 Extended** and **Common Criteria Part 3 Conformant**, and meets the assurance requirements of EAL 2.

Retina Network Security Scanner is an IDS-type product developed by eEye Digital Security Corporation. It is a non-disruptive network security scanner, meaning it is not invasive, nor does it interfere with the operation of the IT system being monitored. The TOE does not scan network traffic anomalies reported by sensors, as do some other types of IDS products. Rather the TOE scans hosts identified within a specific IP range. Ports on targeted hosts are monitored for specific activities and events identified in an audit policy.

The TOE is supported on Microsoft Windows NT 4.0 SP6a, 2000, 2003, and XP.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC, the Retina Network Security Scanner Security Target, and analysis performed by the Validation Team.

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 5, and the Conclusions presented in Section 6 of

the ETR. The validation team therefore concludes that the evaluation and the Pass results for the Retina Security Scanner is complete and correct.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology 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 organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Retina Network Security Scanner, Version 5.4.21.53
ST:	Retina Network Security Scanner Security Target, Version 1.0, 25 May 2007
Evaluation Technical Report	Evaluation Technical Report for eEye Retina Network Security Scanner: • Part 1 (Non-Proprietary), Version 1.0, 25 May 2007 • Part 2 (Proprietary), Version 1.0, 25 May 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2
CEM Version	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.2, January 2004, CCIMB-2004-01-004
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	eEye Digital Security Corporation One Columbia Aliso Viejo, CA 92656
Developer	eEye Digital Security Corporation One Columbia Aliso Viejo, CA 92656
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Ralph Broom, Noblis
	Jerome F. Myers, The Aerospace Corporation

3 Security Policy

The Retina Network Security Scanner enforces the following security policies as described in the Security Target.

> ***Note:*** *Much of the description of the Retina Network Security Scanner security policy has been extracted and reworked from the Retina Network Security Scanner Security Target and Final ETR.*

3.1 Network Security System

The TOE scans hosts identified within a specific IP range against predefined audit policies (that are set at the granularity of a specific host or collection of hosts), to detect known potential vulnerabilities. The audit policies govern the collection of data regarding inappropriate activities on the IT systems the TOE monitors. The TOE collects the following information from targeted IT systems: security configuration changes; access control configuration; service configuration; authentication configuration; accountability policy configuration; and detected known vulnerabilities. The TOE provides the means to search, sort, and order collected Scanner data based on targeted IT System identity, time, and event type, and to generate reports of the results of an audit scan, including detailed remediation reports and summary executive reports.

3.2 Security Management

The Retina Network Security Scanner provides the authorized user with a GUI that can be used to configure and modify the options of the TOE. In particular, the GUI provides the user with the following capabilities: discover target hosts by IP address, IP address range, CIDR notation, or host name; configure and launch audits of discovered hosts, including selecting audit options; review results of audits, including classification of vulnerabilities and other collected data; and generate remediation and summary reports of the results of the audit.

4 Assumptions

The following assumptions underlying the evaluation of Retina Network Security Scanner are identified in the Retina Network Security Scanner Security Target.

4.1 Usage Assumptions

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

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

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

4.2 Physical Assumptions

The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorized physical access.

It is assumed that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 Personnel Assumptions

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

The authorized users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The TOE can only be accessed by authorized users.

4.4 System Assumptions

The TOE operating environment must successfully identify and authenticate users prior to allowing access to TOE functions and data.

The TOE operating environment will provide protection to the TOE and its related data.

The TOE operating environment will provide reliable system time.

4.5 Clarification of Scope

The TOE relies on the underlying operating system and its security. The operating system on which the TOE is installed is outside the TOE and hence its security properties are not covered by this evaluation.

The following product features described in the guidance documentation for the TOE were not covered in the evaluation: use of the Audit Wizard; use of Retina Plug-ins;

configuration of a central policy server; configuration to route events to a REM Event Server; use of Auto-Update (which would take the TOE out of its evaluated configuration); and using a DSN to store collected Scanner data.

5 Architectural Information

Note: *The following architectural description is based on the description presented in Part 1 of the Retina Network Security Scanner ETR and in the Security Target.*

The TOE comprises the following components:

- Scanning Engine
- Scanner Shell.

The Scanning Engine runs as a Windows service. It performs all the scanning operations, based on the configured audit policies. The process of scanning a host occurs essentially in the following manner:

- ICMP ping: This step establishes if the host is responding.
- Target setup: The specific details of the target are built, such as MAC addresses, reverse DNS hostnames and other details.
- Syn Scan: Using a series of TCP syn packets, the TOE scans the host to determine which ports are responding.
- Protocol Detection: Whenever a port is found to be open, after the TOE establishes a connection with the port, it determines the protocol of the service offered on the port using the port number and any protocol-specific information that is initially returned by the target when the connection is established.
- OS Detection: Using a series of packets designed to "fingerprint" the target operating system, the TOE matches the output against a database of known operating systems.
- Audit Phase: The audit phase is effectively the second half of the scan and encompasses the basic vulnerability scan portion of the audit.

It is in the audit phase when the TOE applies the audit policy looking for specific services and protocols for the specific targeted host.

The Scanner Shell (shell) runs as a user mode application and handles all aspects of the local user interface of a scan, such as scan range entry, audit set-up, results display, and reporting.

The Scanning Engine and Scanner Shell communicate via Remote Procedure Call (RPC).

In addition to the GUI provided by the Scanner Shell, the TOE provides two command line interfaces. The user can invoke the GUI from a console prompt, specifying a limited set of command line switches, or can direct the operation of the Scanning Engine using an RPC client (RetRPC_Client.exe) provided as part of the TOE.

The TOE can be installed on machines running Microsoft Windows NT 4.0 SP6a, 2000, 2003, and XP.

6 Documentation

The following documents are provided with the TOE and provide information pertinent to the installation, configuration, and operation of the TOE:

- Retina Network Security Scanner Users Manual, Revision 5-3-1
- Retina Network Security Scanner Release Notes, version 5.4.21.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Retina Network Security Scanner, Version 0.3, 30 May 2007.

7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The developer testing provided coverage of all of the security functions identified in the ST. These security functions are:

- Network Security System
- Security Management.

However, the developer testing covered only the GUI component of the TSFI. The command line interface available for invoking the GUI component and the command line interface provided by the RPC client supplied with the TOE were not covered in the developer testing.

Developer testing was performed only on one of the supported platforms (Microsoft Windows Server 2003 SP1), since there are no code changes for other supported platforms. There is only a single set of installation and runtime TOE components. There are no differences in the services the TOE relies on from the IT Environment provided by the other supported platforms.

7.2 Evaluation Team Independent Testing

The evaluation team test configuration comprised the following computers:

- TOE host:
    - Dell Latitude laptop with Mobile Intel Pentium 4-M 2.20 Ghz CPU, 512 MB RAM, 6 GB HDD

  - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1) (Windows Server 2003 Enterprise Edition)

- Windows target
  - Dell Dimension 370 with Intel Pentium 4 3.40 GHz CPU, 1GB RAM, 150 GB HDD
  - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1) (Windows Server 2003 Enterprise Edition)
- Unix target
  - Sun Microsystems SunBlade 150 with sparc processor, 512 MB RAM
  - Solaris 9 (SunOS Release 5.9 Generic_117171-14).

These computers were connected via a small LAN.

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran 70% of the developer tests and verified the results on the TOE host, then developed and performed functional and vulnerability testing that augmented the developer testing by exercising different aspects of the security functionality.

The evaluation team performed the following additional functional tests:

- Expanded audit and target IT system: The developer's Test Documentation describes testing the scanner functionality of the TOE against an SNMP server (deployed on a virtual machine using VMWare). The evaluation team had access to computers hosting other operating systems (i.e., Solaris 9) and services (DNS, RPC, SSH, SMTP) that the TOE can scan for and audit. The test demonstrated that the TOE could scan computers hosting various operating systems (Windows Server 2003, Solaris 9), identify various services running on those computers, and identify vulnerabilities associated with the computers and their services.
- Scanning with credentials: By default, the TOE runs (and executes its scans of target IT systems) as the LOCAL_SYSTEM user. As described in the Retina Network Security Scanner Users Manual, this user has no access to Windows Networking connections – such as NetBIOS and remote registries. In order to obtain more detailed results, it is necessary to provide the scanner with credentials for the target IT system that will provide the TOE with that access (e.g., 'Administrator', with the correct password). The test demonstrated that the TOE collected additional scanner data when the audit was run using credentials for the target IT system.
- Verifying scanner data review capability: The ST and design evidence claim scanner data review capability that is not covered by the developer's testing. The evaluation team developed a test to assess the claims made in the ST. The test demonstrated that the TOE provides capabilities to search, sort and order collected scanner data based on target system id, time, and event type (vulnerability).

The evaluation team performed the following vulnerability tests:

- Stored credential search: As described above, the TOE runs (and executes its scans of target IT systems) as the LOCAL_SYSTEM user by default. In order to obtain more detailed results, it is necessary to provide the scanner with credentials for the target IT system that will provide the TOE with that access (e.g., 'Administrator', with the correct password). These credentials are stored on the TOE computer in the local LSA store. The evaluation team determined that the stored credentials are not vulnerable to a non-administrative user of the TOE.
- Credential grabbing during a vulnerability scan: The TOE allows authorized users to enter username and password (I&A credentials) of machines to be scanned. The evaluation team attempted to ascertain the password using a network sniffer. The evaluation team determined credentials used in a scan are protected when sent over the network by the TOE.
- TOE installation protection: The TOE relies on the underlying operating system to protect it from tampering and bypass, and to protect the stored scanner data and other configuration data. The evaluation team, operating as an unprivileged user on the TOE computer, attempted to interfere with the operation of the TOE and its data. The evaluation team determined the underlying operating system provides adequate protection to the TOE and its data from unauthorized users.
- RPC exploitation: The TOE uses Remote Procedure Call (RPC) as the means by which the Retina Shell and the RPC client utility communicate with the Scanner Engine. This use of RPC could introduce a vulnerability. The developer provided design details on how RPC is used such that a vulnerability is not exposed. The use of RPC within the TOE does not appear to introduce any obvious vulnerability to the TOE. **Note:** This result applies only to the use by the TOE of RPC for communication between TOE components. It does not imply that the implementation of RPC in the underlying operating system is free from vulnerabilities.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Retina Network Security Scanner Version 5.4.21.53, running on Microsoft Windows NT 4.0 SP6a, 2000, 2003, and XP. To use the product in the evaluated configuration, the product must be installed and configured as specified in the following documentation:

- Retina Network Security Scanner Users Manual, Revision 5-3-1, 4 May 2006
- Retina Network Security Scanner Release Notes, Revision 5.4.21, 8 May 2006.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2 [1]–[5]. The evaluation determined the Retina Network Security Scanner TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements. The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for eEye Retina Network Security Scanner Part 2** which is considered proprietary.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the vendor tests, the evaluation team's independent tests, and the penetration tests also demonstrated the accuracy of the claims in the ST.

Under the Validation Oversight Review (VOR) process, the Validators review EAL2 evaluation evidence twice; at the Initial VOR and the Final VOR. The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

Validator comments and recommendations have been captured in Section 4.5 Clarifications of Scope and other sections.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Retina Network Security Scanner Security Target, Version 1.0, 25 May 2007*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.2, January 2004.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.2, January 2004.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.2, January 2004.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.2, January 2004.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations,* Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for eEye Retina Network Security Scanner Version 5.4.21.53 Part 1*, Version 1.0, 25 May 2007.

[8] Science Applications International Corporation. *Evaluation Technical Report for eEye Retina Network Security Scanner Version 5.4.21.53 Part 2 (SAIC and eEye Proprietary)*, Version 1.0, 25 May 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Report for eEye Retina Network Security Scanner Version 5.4.21.53, ETR Part 2 Supplement (SAIC and eEye Proprietary),* Version 1.0, 25 May 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Science Applications International Corporation. *Retina Network Security Scanner Security Target*, Version 1.0, 25 May 2007.