Certification Report

EAL 2 Evaluation of NIKSUN®, Inc.

NetDetector®/NetVCR® 2005

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-28
Version: 1.0
Date: 03 March 2005
Pagination: i to iv, 1 to 15

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. This certification report and its associated certificate apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Limited located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 03 March 2005, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: NIKSUN, NetDetector and NetVCR which are registered trademarks of NIKSUN®, Inc; Windows 2000 Professional and Internet Explorer which are registered trademarks of Microsoft® Corporation; Pentium and Xeon which are registered trademarks of Intel® Corporation; and Java which is a registered trademark of Sun Microsystems, Inc.

TABLE OF CONTENTS

Executive Summary

The NetDetector®/NetVCR® 2005 from NIKSUN®, Inc. is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The NIKSUN®, Inc. NetDetector®/NetVCR® 2005 appliance is designed to be a non-intrusive network surveillance system that provides the capability to record and analyze traffic streams at high data rates to detect and report on anomalous activities and patterns indicative of security or performance incidents in near real-time or post-event. This feature is the result of a packet capture and recording engine coupled with a query processor. Data captured by the appliance is analyzed to inspect traffic flows for improper activities, detect intruders, and send alerts while continuously recording and analyzing every packet in the network in near-real time. Reconstruction of all network activity at the application layer (e.g., Web activity, E-mail, FTP, Telnet, instant messaging etc.) is available to completely analyze suspicious activity, thus allowing for post-event investigation of a network intrusion.

Once an intrusion has been identified, activities associated with the intrusion can be recreated and traced to identify the source of intrusion, determine what the intruder did, and see how the intruder managed to bypass other security mechanisms. The appliance provides information needed to determine what actions are required to secure the network after a security breach has occurred.

Electronic Warfare Associates-Canada, Limited is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 21 February 2005, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the NetDetector®/NetVCR®, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NetDetector®/NetVCR® are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product indicate that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation,*

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Version 1.0 (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*.

The Communications Security Establishment, as the CCS Certification Body, declares that the NetDetector®/NetVCR® 2005 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is the NetDetector®/NetVCR® 2005, from NIKSUN®, Inc.

2 TOE Description

The NIKSUN®, Inc. NetDetector®/NetVCR® 2005 will passively and non-intrusively record all packets from a monitored network while simultaneously generating and storing multi-level statistics which enable analysis from the link layer to the application layer. The NetDetector®/NetVCR® application modules utilize the data to perform advanced features such as statistical anomaly/Quality of Service detection, security and performance signature detection, application and session reconstruction (web, email, IM, FTP, Telnet), scheduled or on-demand reporting, and multi-format data import/export. A web-based graphical user interface (GUI) provides a convenient standard client access to the management, configuration, and application features.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the NetDetector®/NetVCR® is identified in Section 5.1 TOE Security Functional Requirements of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: NIKSUN®, Inc. NetDetector®/NetVCR® 2005 Security Target
Version: 1.5
Date: 18 February 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*, incorporating all final CC interpretations issued prior to 15 March 2004. The NetDetector®/NetVCR® 2005 is:

a) Common Criteria *Part 2 extended*, with security functional requirements based upon functional components in Common Criteria Part 2 and explicitly-stated security functional requirements for IDS functions and audit data generation;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c) Common Criteria EAL 2 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The developer claimed security policies for the NetDetector®/NetVCR® 2005 are described in this section.

6.1 Identification and Authentication

When accessing the NetDetector®/NetVCR® 2005 through its web GUI, no actions other than HTTPS session establishment are permitted prior to the successful identification and authentication of the user. When accessing the NetDetector®/NetVCR® 2005 through an attached CLI console, no actions are permitted prior to the successful identification and authentication of the user. Password expiration information is associated with each user.

6.2 Security Audit

The audit log of the NetDetector®/NetVCR® 2005, known as the Activities Log, can only be read by Administrators or Advanced Users through the web GUI, or Superusers or Appliance Users through the CLI console. Administrators can create additional web access groups and grant them explicit read access to the Activities Log. No GUI user can directly write to, modify, or delete audit records. The auditing function cannot be disabled by the user.

The NetDetector®/NetVCR® 2005 has a log rotation mechanism to handle logfiles when they reach a certain allowed maximum size. When the number of old Activities logfiles exceeds 4, the NetDetector®/NetVCR® 2005 will delete the oldest log to free up disk space.

6.3 Security Management

The authorized roles that a web GUI user can assume are Administrator, Advanced User, User, or any role specifically created by Administrators. The authorized roles that a CLI console user can assume are Superuser and Appliance User.

Administrators can create new roles and grant them permission to manage some or all of the same security functions and TSF data. User/role account management is only available to Administrators and cannot be granted to other roles.

Advanced Users are not authorized to modify any security function behavior. Users are not authorized to modify any security function behavior, and cannot read packet payloads or reconstructed network traffic.

6.4 Protection of TOE Security Functions

All remote communications through the management interface are secured via HTTPS, which utilizes SSL, protecting data from disclosure as it is transmitted between a web browser and the NetDetector®/NetVCR® 2005.

Traffic recorded by a recording interface is never executed by the NetDetector®/NetVCR® 2005 and is stored in an area of the file system separate from all other TOE data and OS/system binaries.

The system time is initially set during installation and can only be reset by the CLI Superuser.

6.5 Data Collection and Storage

The NetDetector®/NetVCR® 2005 enforces an automatic space management policy whereby the oldest data from the largest recorded data streams is deleted continuously as needed to free up space for new data to be recorded. Data designated as archive data by Administrators is not deleted for space management.

6.6 Data Analysis and Response

The Event Viewer contains a running log of all alarms detected by the Anomaly, Signature, Quality of Service (QoS), and Real Time Experts (RTX) mechanisms. The Event Viewer keeps up to 100,000 of the latest events, and will delete the oldest events to make space for new events after the limit has been reached.

7 Assumptions and Clarification of Scope

Consumers of the NetDetector®/NetVCR® 2005 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the NetDetector®/NetVCR® 2005.

7.1 Secure Usage Assumptions

a. The NetDetector®/NetVCR® 2005 will be properly installed and configured according to guidance documentation.

b. The TOE will only be accessed by authorized users.

c. Individuals assigned as authorized administrators to manage the TOE, and the security information it contains, are competent.
d. An authorized administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

a. The NetDetector®/NetVCR® 2005 will be located within a controlled access facility, intended to prevent unauthorized physical access.
b. The management interface of the NetDetector®/NetVCR® 2005 will be connected to a secured, separate network from the recording interfaces.
c. The TOE has access to all the IT System data it needs to perform collection, analysis, detection, storage, and presentation of network traffic.
d. The TOE is appropriately scalable to the IT Systems it monitors.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

The NetDetector®/NetVCR® 2005 does not readily present audit logs of actions performed through the CLI console thus it may be possible for attacks made by an authorized local administrator that has direct access to the TOE to go unnoticed. Console access is intended only for initial installation and troubleshooting.

The NetDetector®/NetVCR® 2005 does not readily present logs for the disconnection of the network it is monitoring, therefore the inadvertent or deliberate disconnection of the monitored network, and the possible misuse of the monitored network during this time, may go undetected.

As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or "vulnerabilities" to objectives not claimed in the ST.

8 Architectural Information

The NetDetector®/NetVCR® 2005 is comprised of the following subsystems:

a. Data Capture Engine (DCE):
Provides the core platform that collects data packets from tapped networks and stores them to disk. It simultaneously computes statistical metadata and stores that information to disk as well. Executables to query the data are also included as part of the DCE.

The DCE is based on a custom-built, hardened version of the FreeBSD operating system. In addition to the network interface cards and other device drivers, the OS provides such

services as boot-up, initialization, file system, process scheduling, auditing, time stamps, and TCP/IP stack and protocol implementation.

b. User Interface Engine (UIE):
Includes sub-components such as the Apache web server, CGI engine, servlet engine, and applets. Screens related to Configuration, Traffic Analysis, Event Viewing, and Data Management are under direct control of the UIE. The UIE is also responsible for the main Identification and Authentication, Security Management, and Audit Review functionality.

c. NetDetector® Application Modules:
The NetDetector® Application Modules examine captured packets for security considerations. The modules are: Anomaly Detection, Signature Detection, and TCP Application Reconstruction.

The Anomaly Detection module will track and provide alerts based on statistical thresholds defined by authorized users. It will take query results from the DCE and yield output for rendering by the UIE in the Event Viewer. It can also produce alerts via SMTP mail messages and SNMP traps.

The Signature Detection module takes query results from the DCE (raw packet data), looks for specific patterns for which to provide alerts, and presents its output in the Event Viewer or to an external syslog server.

The TCP Application Reconstruction module has the capability to arrange and reassemble payload data from packets in TCP sessions and display them in various forms (e.g., ASCII, hex, raw rendering). Data is interpreted through the state machines of selected applications (E-mail, Web, FTP, IM, and Telnet) for application specific viewings.

d. NetVCR® Application Modules:
The NetVCR® Application Modules examine the performance of a network. The modules are: NetSLM (Quality of Service) and Real Time Experts (NetRTX).

The NetSLM module computes performance statistics such as the number of bytes, the number of packets, the network utilization, and the bit rate for packet data streams and provides notification of triggered alarms. The alarms are based upon user-defined thresholds that are exceeded or not met.

The NetRTX module looks for particular performance-relevant patterns within packets. If a particular pattern is found, NetRTX provides notification to the Event Viewer and optionally sends the notification to a trusted syslog server or trusted SNMP trap receiver.

e. Data Import/Export Subsystem:
This subsystem consists of export and import utilities. Export writes data in the form of datasets from the database into a transportable operating system file. Import reads data from such files back into the database.

9 Evaluated Configuration

The evaluation used the following NetDetector®/NetVCR® 2005 appliance with NetDetector®/NetVCR® 2005 build 3.1sp2_3 software running on it:

- A 2U appliance (NKN-2411-FE-2HDX-292 featuring dual CPUs, minimum 2 GB RAM, 10/100 Ethernet Management Interface, CD-ROM and Floppy Drives with minimum 292 GB storage configured for monitoring 2 HDX Fast Ethernet links)

The two particular NetDetector®/NetVCR® 2005 appliance configurations tested were the following:

- NetDetector®/NetVCR® 2005 build 3.1sp2_3 software

  running on either:

  a. a 2U IBM xSeries 345 Dual 2.4 GHz Xeon Processor 4 X 73 GB SCSI drives 2 GB RAM with dual port FastE NIC;

     or

  b. a 2U Intel Server SE7500WV2 M.B 2 GB RAM Dual P3 XEON CPU 4 X 73 GB HDD with dual port FastE NIC

Configuration details of evaluated configuration:

- All network services except HTTPS are disabled.

Environment of TOE:

- CLI was achieved through a directly connected PS/2 keyboard and VGA monitor as the console; and
- GUI communication through Internet Explorer® 6.0 browser with JRE 1.4.1 on Microsoft® Windows 2000® Professional SP4 running on a 3.0 GHz Pentium® 4 PC.

10 Documentation

The documentation provided with the NetDetector®/NetVCR® 2005 appliance includes the following:

1. *NIKSUN® NetDetector/NetVCR® Version 2005 User's Guide*, January 25, 2005 (electronic copy);

   - administrator and user guidance for secure usage of the NetDetector®/NetVCR® 2005 appliance

2. *NIKSUN® Appliance Customer Installation Guide Version 2005*, May 28, 2004 (printed and electronic copies)

   - complete installation instructions

3. *NIKSUN® NetDetector® Installation Instructions Version 2005*, October 12, 2004 (electronic copy)

   - software update installation instructions

4. *NetDetector 2005: ReadMe First* (printed and electronic copies); and

5. *NIKSUN NKN-2400 Quick Start User Guide* (printed copy)

   - hardware installation information.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the NetDetector®/NetVCR® 2005, including the following areas:

Configuration management: An analysis of the NetDetector®/NetVCR® 2005 development environment and associated documentation was performed. The evaluators found that the NetDetector®/NetVCR® 2005 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the

NetDetector®/NetVCR® 2005 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluator analysed the NetDetector®/NetVCR® 2005 functional specification and high-level design and determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluator also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the NetDetector®/NetVCR® 2005 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The NetDetector®/NetVCR® 2005 ST strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability and strength of function analyses. In addition, the evaluators performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in the NetDetector®/NetVCR® 2005.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

ITS product testing at the EAL 2 level of assurance includes the following in regards to the developer's testing: examination of the developer's test plans, test procedures and test results; evaluation of the developer's test coverage analysis in regards to the functional specification for the TOE, and witnessing the execution of the some of the developer's tests. The evaluators conduct independent functional testing to prove the claimed security functionality taking into consideration the developer's test coverage and conduct penetration and vulnerability testing, taking into consideration the developer's vulnerability assessment, but also obvious publicly-known vulnerabilities to which the TOE may be susceptible. Vulnerability testing is dependent on the intended environment for the usage of the TOE.

12.1 Assessing Developer Tests

The evaluators verified that NIKSUN meets its testing responsibilities by devising and documenting test plans which included test configuration information and devising and documenting repeatable test cases. Bugs or errors found during testing were tracked and resolved.

NIKSUN fully tests its releases with developers performing unit testing on individual modules and testers performing integration, feature, penetration and system testing. NIKSUN extensively tested the primary IT security functionality of the NetDetector®/NetVCR® 2005 and covered some of the secondary IT security functionality of the NetDetector®/NetVCR® 2005.

NIKSUN also performs sanity checks on all appliance hardware it receives from third party vendors before preparing the NetDetector®/NetVCR® 2005 appliances for shipping.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation and examining the developer's test documentation. The evaluator executed a large sample of the developer's test cases and created test cases that augmented the developer tests.

The evaluator's functional testing focused on the following objectives:

a. Testing of the installation of the NetDetector®/NetVCR® 2005;

b. Repeating NIKSUN tests that were not witnessed;

c. Testing identification and authentication claims;

d. Testing of the audit functionality of the NetDetector®/NetVCR® 2005;

e. Testing of the account management functionality of the NetDetector®/NetVCR® 2005;

f. Testing of domain separation claims;

g. Boundary testing of the external interfaces of the NetDetector®/NetVCR® 2005; and

h. Verifying strength of function claims.

12.3 Independent Penetration Testing

During this evaluation, the evaluator developed independent penetration tests using the following developer sources of information for the NetDetector®/NetVCR® 2005: the developer's vulnerability analysis, the ST, the functional specification, the high-level design, and the installation, user and administrator guidance. The evaluator used the following publicly-available sources of information as well: websites for component bug reports, the Common Vulnerabilities and Exposures website, @stake, CERT Coordination Center, US Department of Energy, NIST, ICAT Metabase, CanCERT, and Bugtraq Security Focus.

The penetration tests focused on the following:

a. Generic vulnerabilities;

b. Bypassing;

c. Tampering;

d. Direct attacks; and

e. Misuse.

12.4 Conduct of Testing

The NetDetector®/NetVCR® 2005 was subjected to a comprehensive suite of formally-documented, independent functional and penetration tests. The testing took place at the NIKSUN®, Inc.'s facility in Monmouth Junction, New Jersey and the ITSET facility at Electronic Warfare Associates-Canada, Limited located in Ottawa, Ontario. The Canadian Common Criteria Evaluation and Certification Scheme (CCS) Certification Body (CB) witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the Evaluation Technical Report (ETR)[2].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the NetDetector®/NetVCR® 2005 behaves as specified in its ST and functional specification. The functional and penetration testing resulted in a **PASS** verdict.

The only vulnerability the evaluator was able to exploit in the intended environment for the NetDetector®/NetVCR® 2005 was access to some user data such as reports and FTP packet data through the management GUI without being identified and authenticated to the NetDetector®/NetVCR® 2005. This is considered to be a residual vulnerability (beyond EAL2) and was targeted by the developer to be fixed in the next release.

[2] The Evaluation Technical Report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The evaluators found the installation, user and administrator guidance for the NetDetector®/NetVCR® 2005 to be comprehensive; the configuration management and secure delivery procedures implemented by NIKSUN to be of sufficient thoroughness to ensure that the consumer receives the expected product, and that NIKSUN extensively quality tests the primary security functionality of the NetDetector®/NetVCR® 2005 appliances.

The evaluators recommend that consumers ensure that the management network for the NetDetector®/NetVCR® 2005 is separate and secure to mitigate the residual vulnerability of unauthenticated access to some user data. Also, the evaluators indicate that it is important that procedures are in place to restrict physical access to the NetDetector®/NetVCR® 2005.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
ASCII	American Standard Code for Information Interchange
CanCERT	Canadian Computer Emergency Response Team
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CD-ROM	Compact Disc-Read Only Memory
CEM	Common Methodology for Information Technology Security Evaluation

CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CLI	Command Line Interface
CPU	Central Processing Unit
CR	Certification Report
CSE	Communications Security Establishment
DCE	Data Capture Engine
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FastE	Fast Ethernet (10/100 Mbits per second)
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HDD	Hard Disk Drive
HDX	Half-Duplex
HTTPS	Secure Hypertext Transfer Protocol
IDS	Intrusion Detection System
IM	Instant Message
ISO	International Organisation for Standardisation
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
JRE	Java™ Runtime Environment
Mbits	Megabits
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
PC	Personal Computer
PS/2	Personal System 2 keyboard
QoS	Quality of Service
RAM	Random Access Memory
RTX	Real Time Experts
SCSI	Small Computer System Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
syslog	Microsoft® Windows system log
TCP	Transmission Control Protocol
TOE	Target of Evaluation

UIE	User Interface Engine
VGA	Video Graphics Array
2U	Two Unit Rackmount Server Size

Note: ICAT was an acronym for a NIST project initially intended as a database of Internet attacks used by hackers but the acronym is obsolete and has no relevant meaning in its current context.

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) *NIKSUN®, Inc. NetDetector®/NetVCR® 2005 Security Target*, Document ID: NK-CC-ST-NDV2005-1.5, Version 1.5, 18 February 2005.

e) *Evaluation Technical Report (ETR), NIKSUN®, Inc. NetDetector®/NetVCR® 2005 EAL 2 Evaluation*, Document No. 1472-000-D002, Version 1.2, 2 March 2005.