National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

NCR

Teradata® Database V2R5.0.2

Report Number: CCEVS-VR-04-0073

Dated: 11-October 2004

Version: 1.1

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

Validator

John Nilles

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Booz-Allen & Hamilton, Inc. Common Criteria Testing Laboratory

Linthicum, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the evaluation of the NCR Teradata® Database V2R5.02. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Booz-Allen & Hamilton (BAH), Incorporated, and was completed during August 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by BAH. The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant,** and meets the assurance requirements of **EAL 2**. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfy the needs for protection of sensitive information as defined by DoD Standard 8500.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is the Teradata® RDBMS V2R5.0.2 The TOE accesses, stores, and operates on data using Teradata® Structured Query Language (Teradata® SQL), which is compatible to ANSI SQL with extensions. The TOE was developed to allow users to view and manage large amounts of data as a collection of related tables. The Teradata® RDBMS V2R5.0.2 enforces a discretionary access control policy such that the owner of a database object or resource (databases, tables, views, stored procedures and macros) has the authority to permit an authorized user access to those objects or resources.

This evaluation was scoped to a subset of the Teradata® database system, which excluded hardware and selected portions of the Teradata® Database software. Section two (2) of the security target provides specific details of that scope.

The validator monitored the activities of the BAH evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The validation team determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the BAH findings are accurate, the conclusions justified, and the conformance claims 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 EAL 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~~Table 1~~ provides information needed to completely identify the product, including:

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Teradata® Database V2R5.0.2
Protection Profile	None
Security Target	Teradata® Relational Database Management System Version 2, Release 5.0.2 Security Target (Version 1.0) dated October 11, 2004.
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation – Teradata® Relational Database Management System Version 2, Release 5.0, ETR Version 1.4, dated October 11, 2004
Conformance Result	Part 2 extend and Part 3 conformant, EAL 2
Sponsor	NCR
Developer	NCR
Evaluators	Booz-Allen & Hamilton (BAH), Incorporated
Validator	The Aerospace Corporation

3. SECURITY POLICY

The Teradata® Database V2R5.0.2 enforces the following security policies:

3.1. Security Audit

The TOE provides auditing/logging functions to record Trusted Security Function (TSF) security relevant events on the hard drive of the local server. Teradata® RDBMS V2R5.0.2 uses a set of rules stored in the system table DBC.AccLogRuleTbl to determine whether an access request requires an audit record to be generated. If so, the Database writes the resulting event(s) to the system audit table, DBC.AccLogTbl, which is generated during installation.

Searching and sorting audit data is done with SQL statements, and can be done by any user with access rights to the DBC.AccLogTbl. In addition to directly querying the access log table with SQL, authorized users can use the friendlier interface provided with the Teradata® Manager. As with any SQL query, the results set can be ordered by any of the table's columns, which include such fields as LogDate, LogTime, LogonDate, LogonTime, UserName, DatabaseName, etc.

The user(s) accessing the audit information must have access rights to the DBC.AccLogTbl. At installation, only the DBC user has these rights, this user grants access only to the security administrator. No other users will have access to read or delete access log table entries.

3.2. Identification and Authentication

Database user identification and authentication is performed by the session controller module. The requirement for a password (and its strength) is controlled through the user's assigned profile, which the administrator configures. The Teradata® RDBMS V2R5.0.2 provides for several configurable controls related to password authentication. The following security administrator configurable controls combine to satisfy the requirements regarding passwords:

- Maximum Logon Attempts (with incorrect password)
- Minimum Characters in a Password
- Password Lockout Time

The TOE does not require that a profile be assigned to every user, but if there is no profile assigned, then default security attributes defined in the SysSecDefaults table apply.

3.3. Security Management.

The Teradata® database is administered via SQL and/or the Console Database Window (CDW). The security administrator is responsible for setting Teradata® security parameters to match the local policy. This includes setting the audit policy, setting the identification and authentication parameters, setting database object security attributes, managing roles, and setting limits on resources to prevent exhaustion.

For detailed information on managing specific policies, configurations, etc., refer to the administrative guidance documents identified in section six of this document.

3.4. Discressionary Access Control

The Teradata® Database implements a discretionary access control mechanism through which users and/or the security administrator can limit access to database objects. The rights to a database object are initially vested in the owner of the object when the object is created. Each object type (e.g., table, database macro) has a predefined set of rights that are granted. The owner can then use SQL GRANT/REVOKE statements to pass these rights on to other users directly, or the rights can be passed to a ROLE and then the use of that role can be given to a set of users. The database objects that conform to the access control policy stated in section 5.1.2.2 of the ST are databases, tables, views, macros and stored procedures.

3.5. Resource Utilization

The Database enforces administratively controlled maximum quotas on various resources to ensure that tables are protected from invalid events that could encroach on valid events. Resources that may be limited via quotas include CPU time, logical disk blocks, and allocated database storage.

4. ASSUMPTIONS

4.1. Usage Assumptions

The Teradata® database is installed configured and administered in accordance with the evaluated configuration guidance.

The Teradata® database administrator is competent and trusted not to abuse his/her privilege.

4.2. Environmental Assumptions

The Teradata® database server is located in a physically protected, secure facility in order to prevent physical access to the TOE by anyone other than authorized personnel.

The Teradata® database server is protected by a firewall that has been configured to mitigate malicious attacks against the operating system upon which the TOE operates.

Any other IT components with which the Teradata® database communicates are assumed to be under the same management control and operate under the same security policy.

5. ARCHITECTURAL INFORMATION

The Teradata® RDBMS is a complete relational database management system. Teradata® was developed to allow users to view and manage large amounts of data as a collection of related tables.With the Teradata® RDBMS, one can access, store, and operate on data using Teradata® Structured Query Language (Teradata® SQL), which is compatible to ANSI SQL with extensions.

The TOE is comprised of several components including the Parallel Database Extension (PDE), Gateway for LAN, Parsing Engine (PE) and the Access Module Processor (AMP). See

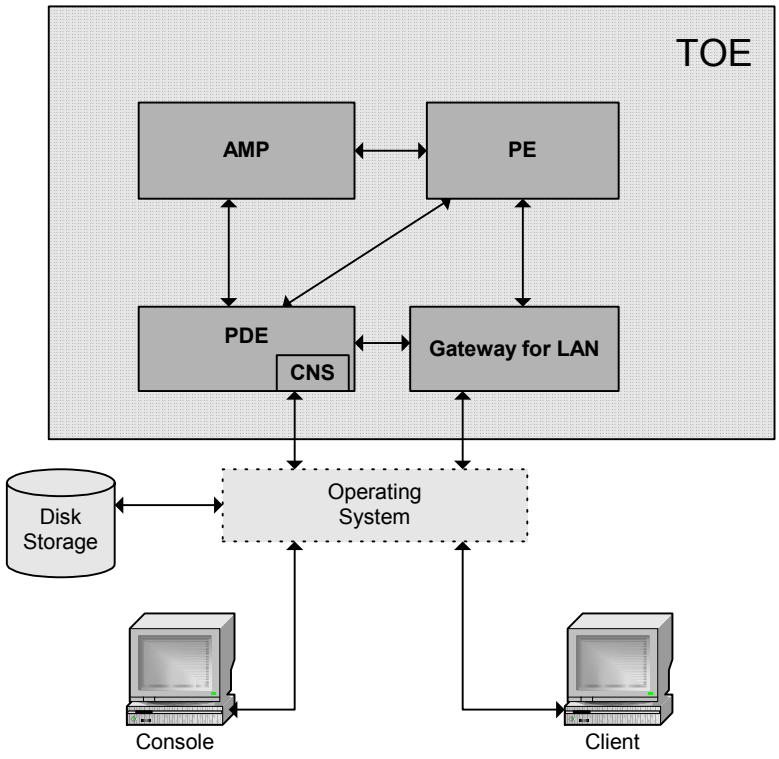

Figure 1 Teradata® RDBMS Archecture

5.1. Parallel Database Extension

The Parallel Database Extension element is a software interface layer that operates on top of the host Operating System (OS), thus providing an interface between the TOE and the underlying OS software. The PDE includes a BYNet Driver that manages the communication devices that interconnect the hardware nodes on which the server software is resident. It provides a standard interface for inter-process communications across nodes in a multi-node environment.

In addition, the PDE is responsible for starting all tasks defined in the PE and AMP components. Therefore, if a foreign application were executing on a server node and attempted to call a PDE function that call would be rejected.

5.2. Gateway for LAN

The function of the Gateway for LAN element is to provide the client communications interface over the LAN. It receives all messages sent from the client to the server. This includes not only messages containing Teradata® SQL statements but also messages for functions such as connecting and disconnecting sessions, determining the configuration of the server, establishing the security protocols to be used between the client and server, and responding to test messages that determine the health of the server over the LAN.

When the Gateway for LAN receives messages from the client that contain Teradata® SQL requests, it checks those messages to ensure they conform to the specified protocol. Then, those messages are forwarded to the other components within the PE. In addition, the Gateway for LAN receives response messages from the PE, and returns them to the appropriate client.

The Gateway for LAN also interacts with PDE in order to utilize OS services. It also utilizes the PDE for memory management and message handling functions.

5.3. Parsing Engine

The PE component is the interface between the client application and the server. The PE contains three subcomponents which are:

- Session Control which processes external requests to establish or terminate a logical connection or session between the application and the server.

- Parser which processes external requests containing Teradata® SQL. The Parser syntactically and semantically processes the SQL statements and prepares an execution plan to process the statement.

- Dispatcher which processes external requests to asynchronously abort a SQL request that is in process for the application, to return blocks of response data from the server to the application or to discard response data sets maintained in the server.

5.4. Access Module Processor

The AMP component processes the steps of the execution plan prepared by the Parser from a SQL request. The AMP consists of two subcomponents:

- AMP Worker Task (AWT) which receives and processes the steps of an execution plan from the dispatcher subcomponent of the PE. An example of step processing would be to convert the input data received from the client into internal row format, constraint check the data if necessary and then to pass the row to the other AMP subcomponent which is the file system.

- File System subcomponent which is responsible for maintaining the disk resident structure of the relational tables managed by the Teradata® server. The File System receives rows generated by the AWT subcomponent and places them in disk blocks. It interacts with PDE to read and write these blocks to and from disk. It also maintains a B-Tree structure on disk which provides for direct accesses to rows within disk blocks.

6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of the Teradata® Database Version 2 release 5.0.2.

Assuranc Class/Component	Document(s)
ACM_CAP.2: Configuration items	(1) Software Configuration Management (SCM) CMM Practices, March 2001 – 541-0001722-B02 (2) ClearCase Labeling & Branching Standards, March 2003 – 007-0005448-B02 (3) User Guide for ClearCase DBS Development Toolset – 541-0000152-A02 (4) Configuration Item List: • 5.0.2_config.spec.txt • 5.0.2_source.txt
ADO_DEL.1: Delivery procedures	(1) IPP Quality Check Process, Process No. 1231, Revision No. 001 (2) Procedure for Sub Assembly – 541-0004676-A01 (3) Shipping Procedure – 541-0004677-A01 (4) NCR Teradata® Staging Specification Form, Updated 01 September 2003 (5) pkglist.txt (6) Order Summary, 63059655.xls (7) TWF Maintenance Certification pcitpaW2K702.txt
ADO_IGS.1: Installation, generation, and start-up procedures	(1) Teradata® RDBMS Release Summary V2R5.0.2 – B035-1098-122A (2) Base System Release Definition V2R5.0.2, October 2003 – B035-1725-093K (3) Upgrading to V2R5.0.2 for W2K, August 2003 – B035-1113-122K (4) WorldMark 4950/5350 Node Software Installation Guide for Microsoft® Windows® 2000 – B035-5540-083K (5) WorldMark® 4475 Software Installation Guide for Microsoft® Windows® 2000 – B035-5913-083K (6) WorldMark® 4455 Software Installation Guide for Microsoft® Windows® 2000 – B035-5902-123E (7) Parallel Upgrade Tool (PUT) for Microsoft® Windows® 2000 User Guide Release 2.0.4 – B035-5710-122K (8) Teradata® RDBMS Security Administration – B035-1100-122A

Assuranc Class/Component	Document(s)
ADV_FSP.1: Informal functional specification	(1) High Level Design Teradata® Server Architecture Overview, November 2003 – 541-0004657-A03 (2) Teradata® Server Functional Specification, May 11, 2004 – 541-0004655-A03 (3) Introduction to Teradata® RDBMS V2R5.0.2 – B035-1091-122A (4) Teradata® Call-Level Interface Version 2 Reference for Channel-Attached Systems – B035-2417-122A (5) Teradata® Call-Level Interface Version 2 Reference for Network-Attached Systems – B035-2418-122A (6) Teradata® Director Program (TDP) Reference December 2002 – B035-2416-122A (7) Teradata® RDBMS Messages, December 2002 – B035-1096-122A (8) Teradata® RDBMS SQL Reference (Vols. 1,2,4,6) – B035-1101-122A
ADV_HLD.1: Descriptive high-level design	(1) High Level Design Teradata® Server Architecture Overview, November 2003 – 541-0004657-A03 (2) Teradata® Server High Level Design, May 11, 2004 – 541-0004656-A03 (3) Intro to Teradata® RDBMS V2R5.0.2 – B035-1091-122A (4) Teradata® Call-Level Interface Version 2 Reference for Channel-Attached Systems – B035-2417-122A (5) Teradata® Call-Level Interface Version 2 Reference for Network-Attached Systems – B035-2418-122A (6) Teradata® Director Program (TDP) Reference, December 2002 – B035-2416-122A (7) Teradata® RDBMS Messages, December 2002 – B035-1096-122A
ADV_RCR.1: Informal correspondence demonstration	(1) High Level Design Teradata® Server Architecture Overview, November 2003 – 541-0004657-A03 (2) Teradata® Database EAL2 CC Evaluation Representation Correspondence, August 2, 2004 – 541-0004678-A03

Assuranc Class/Component	Document(s)
AGD_ADM.1: Administrator guidance	(1) Teradata® RDBMS Database Administration V2R5.0.2 – B035-1093-122A (2) Teradata® RDBMS Security Administration V2R5.0.2 – B035-1100-122E (3) Teradata® RDBMS SQL Reference (Vols. 1,2,4,6) – B035-1101-122A (4) Teradata® RDBMS Database Window V2R5.0.2 – B035-1095-122A (5) Introduction to Teradata® RDBMS – B035-1091-122A (6) Teradata® RDBMS Database Design – B035-1094-122A (7) Teradata® RDBMS Utilities (Vols. 1, 2, 3) – B035-1102-122A (8) Teradata® RDBMS Data Dictionary V2R5.0.2 – B035-1092-122A (9) Teradata® RDBMS Performance Optimization V2R5.0.2 – B035-1097-122A (10) Teradata® Archive/Recovery Utility Reference Release 07.00.00 – B035-2412-122A (11) Teradata® Manager User Guide Release 6.0 – B035-2428-122A (12) Teradata® Index Wizard User Guide Release 1.00.00 – B035-2506-122A (13) A Guide to Securing Microsoft Windows 2000, Version 1.1, August 26, 2004
AGD_USR.1: User guidance	(1) User Guidance Recap, October 2003 – 541-0004679-A01
ATE_COV.1: Evidence of coverage	(1) Teradata® Server EAL2 CC Evaluation System Test Overview, July 7, 2004 – 541-0004842-A03
ATE_FUN.1: Functional testing	(1) Teradata® Server EAL2 CC Evaluation Test Execution Results, July 13, 2004 – 541-0004879-A01 (2) Teradata® Server EAL2 CC Evaluation System Test Overview, July 7, 2004 – 541-0004842-A03 (3) Teradata® Server EAL2 CC Evaluation Test Suite 1, July 6, 2004 – 541-0004843-A03 (4) Teradata® Server EAL2 CC Evaluation Test Suite (Suites 2, 3, 4), December 17, 2003 – 541-0009999-A01 (5) Teradata® Server EAL2 CC Evaluation Test Suite 5, July 6, 2004 – 541-0004847-A03
ATE_IND.2: Independent testing	(1) Teradata® Server EAL2 CC Evaluation Test Execution Results, July 13, 2004 – 541-0004879-A01 (2) Teradata® Server EAL2 CC Evaluation System Test Overview, July 7, 2004 – 541-0004842-A03 (3) Teradata® Server EAL2 CC Evaluation Test Suite 1, July 6, 2004 – 541-0004843-A03 (4) Teradata® Server EAL2 CC Evaluation Test Suite (Suites 2, 3, 4), December 17, 2003 – 541-0009999-A01 (5) Teradata® Server EAL2 CC Evaluation Test Suite 5, July 6, 2004 – 541-0004847-A03
AVA_SOF.1: Strength of TOE security function evaluation	(1) Teradata® Strength of Function Analysis, September 21, 2004 – 541-0004942-A02
AVA_VLA.1: Developer vulnerability analysis	(1) Teradata® Database EAL2 CC Evaluation Vulnerability Analysis, June 4, 2004 – 541-0004834-A02

7. IT PRODUCT TESTING

7.1. Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[1]

The vendor testing was extensive covered all of the security functions identified in the ST. These security functions include:

- TOE Access
- Identification and Authentication
- User Data Protection
- Security Audit
- Security Management
- Resource Utilization
- Protection of the TSF

7.2. Evaluator Independent Testing

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

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

8. EVALUATED CONFIGURATION

The evaluation configuration consists of the Teradata® Relational Database Management System Version 2, Release 5.0.2. The evaluated configuration requires that:

- The TOE IT environment (the server hardware/windows 2000 operating system) provide the timestamp used for audit events.
- The TOE be installed following the guidance in the *WorldMark® 4455 Software Installation Guide for Secure Locations using Microsoft® Windows® 2000* and *A Guide to Securing Microsoft Windows 2000 For Teradata® Database Environments.*
- Physical access to the TOE be limited to trusted administrators of the TOE.
- The network where the TOE is deployed must be protected by a firewall that has been configured to mitigate malicious attacks against the Operating System upon which the TOE operates.[2]

[2]The *Teradata Position Statement Regarding the Use of Firewalls*, documents two recommended firewall configurations.

9. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable National and International Interpretations in effect on 16 April 2002. The evaluation confirmed that the product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL2. The details of the evaluation are recorded in the Evaluation Technical Report for a Target of Evaluation – Teradata® Relational Database Management System Version 2, Release 5.0. The product was evaluated and tested against the claims presented in the Teradata® Relational Database Management System Version 2, Release 5.0 Security Target (Version 1.0) *dated* October 11, 2004.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation team's results are correct and complete.

9.1. Evaluation of the Teradata®Relational Database Management System Version 2, Release 5.0 Security Target (Version 1.0) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the Teradata® RDBMS that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation.

9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during that process. It is important to note that installation of the Teradata® Database is performed by the vendor's representative and not the end user (purchaser) of the TOE.

9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

9.8. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's rerun of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10. VALIDATOR COMMENTS

The validator observations support the evaluation teams conclusion that the Teradata® Relational Database Management System Version 2, Release 5.0.2 meets the claims stated in the Security Target. The validator also wishes to emphasize that this evaluation excluded hardware, and the operating system upon which the Teradata® Database is installed. Like most application programs, the database is depends upon the secure operation of these underlying systems. Therefore care must be taken to ensure that these underlying system are installed and operated securely. Two documents have been provided to assist Teradata® Database administrators in performing this task: *A Guide to Securing Microsoft Windows 2000 For Teradata® Database Environments* and the *Teradata® Position Statement Regarding the Use of Firewalls*.

11. SECURITY TARGET

Teradata® Relational Database Management System Version 2, Release 5.0.2 Security Target (Version 1.0) *dated* October 11, 2004 is included here by reference.

12. GLOSSARY

Acronym	Description
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol
URL	Uniform Resource Locator

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.