National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme



Common Criteria Evaluation and Validation Scheme Validation Report

McAfee Corporation's Vulnerability Manager Version 7.0

Report Number: CCEVS-VR-VID10461-2011 Version 1.0

Dated: 24 October 2011

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

Jerome F. Myers James Brosey

Common Criteria Testing Laboratory COACT CAFÉ Laboratory Columbia, Maryland 21046-2587

Table of Contents

1	Exe	cutive Summary	4
2	lder	itification	6
2.1	Α	pplicable Interpretations	7
3		Description	
4		umptions	
5		eats	
6		urity Policies	
7		ification of Scope	
8			
		hitecture Information	
9		duct Delivery	
10		roduct Testing	
10.1		valuator Functional Test Environment	
10.2	F	unctional Test Results	22
10.3	Е	valuator Independent Testing	22
10.4	Е	valuator Penetration Tests	22
11		dator Comments	
12		urity Target	
13		of Acronyms	
14		iography	 27
Figure	<u>.</u> 1 -	List of Figures Test Configuration/Setup	17
i iguic	, ,		
-		List of Tables	
Table Table		Evaluation Identifier	
Table		Threats	
Table		Organizational Security Policies	
Table		Test Configuration Overview	
Table		Enterprise Manager Minimum Requirements	
Table		Foundstone Database & Report Server Minimum Requirements	
Table	8 -	Scan Engine Details	
Table	9 -	Web Browser Host Details	20
Table		Additional Host 2 & Attack PC Details	20
Table		Active Directory & DNS Server Details	
Table		Additional Host 1 PC Details	
Table		Additional 3 Host PC Details	
Table	14 -	Additional 4 Host PC Details	21

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the McAfee Corporation's Vulnerability Manager Version 7.0 at EAL2 augmented with ALC_FLR.2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 24 October 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 3.1, Revision 2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the McAfee Corporation's Vulnerability Manager Version 7.0.

The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and misconfiguration. It provides a management interface to configure the system and generate reports regarding the results of the scans.

The TOE consists of the following components:

- Enterprise Manager Component The Enterprise Manager provides authorized users
 with access to the TOE through their Web browsers. It allows them to manage and
 run the TOE from anywhere on the network. Access is protected by user
 identification and authentication.
- Scan Engine Component One or more Scan Engines scan the network environment.
 Depending on the logistics and size of your network, you may need more than one Scan Engine to scan the network. The Scan Engine performs identification, interrogation, and vulnerability assessment of remote computer systems.
- Scan Controller Component The Scan Controller provides the communication between the scan engine and the database. Large or segmented networks (WANs) may require more than one scan controller to be deployed.
- API Service The API service provides an interface for Enterprise Manager to store data into and retrieve data from the Foundstone Database. This interaction uses SOAP over SSL.
- 5. Data synchronization service The Data Synchronization Service enables Vulnerability Manager to import asset information from McAfee's ePO enterprise management system or an LDAP directory such as Microsoft Active Directory. This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.
- 6. Foundstone Database The Foundstone Database is the data repository for the Vulnerability Manager system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and Scan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.
- 7. **Report Server** The Report Server is responsible for generating reports requested by

- authorized users. It retrieves scan results from the Foundstone Database, prepares the report, and saves it for future review.
- 8. **Web Application Scanner** The Web Application Scanner provides a scan configuration, vulnerability checks, and scan reports for web applications. The web application scanner module is a licensed item which can be purchased and added on to a Vulnerability Manager v7.0 deployment at any time. Any scan engine is capable of web application scanning once the module has been purchased with no additional software required.

All communication between distributed components uses a trusted channel to protect the integrity and confidentiality of the data during transit. The TOE depends on cryptographic and protocol functionality provided by the IT environment for these secure channels.

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 desire 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 CCEVS' 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 Identifier

	Table 1 - Evaluation identifier		
McAfee Vulnerability Manager V	McAfee Vulnerability Manager Version 7.0		
Evaluation Scheme	United States NIAP Common Criteria Evaluation and		
	Validation Scheme		
TOE	McAfee Vulnerability Manager Version 7.0		
Protection Profile	N/A		
Security Target	McAfee Corporation's Vulnerability Manager Version 7.0 Security Target Version 0.8, October 21, 2011		
Evaluation Technical Report	Evaluation Technical Report McAfee Vulnerability Manager Version 7.0, Document No. E2-0511-022, Dated August 24, 2011		
Conformance Result	Part 2 Extended and EAL2 Part 3 Conformant Augmented with ALC_FLR.2		
Version of CC	CC Version 3.1, Revision 3 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on December 19, 2008.		
Version of CEM	CEM Version 3.1 and all applicable NIAP and International Interpretations effective on December 19, 2008.		
Sponsor	McAfee, Inc. 2821 Mission College Blvd.		

McAfee Vulnerability Manager Version 7.0	
	Santa Clara, CA 95054
Developer	McAfee, Inc.
	2821 Mission College Blvd.
	Santa Clara, CA 95054
Evaluator(s)	COACT Incorporated
	Greg Beaver
	Jonathan Alexander
Validator(s)	NIAP CCEVS
	Jerome F. Myers
	James Brosey

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3 I-0426 – Content of PP Claims Rationale

I-0427 - Identification of Standards

International Interpretations

None

3 TOE Description

McAfee Vulnerability Manager helps organizations identify and protect their assets by detecting vulnerabilities on their assets. This solution allows managers to continuously monitor, respond, and adjust to a changing risk environment.

Administrators configure the system, including user accounts. Users schedule discovery scans to identify the systems on the network, followed by assessment scans to determine the vulnerabilities.

4 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

Table 2 - Assumptions

	1 100 0 1111
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

5 Threats

The threats identified in the following table sections are addressed by the TOE and/or Operating Environment. The following threats are addressed by the TOE and IT environment, respectively.

Table 3 - Threats

Table 3 - Threats		
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.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.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.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.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source.	
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources.	
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.	
T.FALACT	Issues resulting from scans of monitored systems may fail to be acted upon because the information is not disseminated from the TOE to other IT systems that are responsible for tracking or correcting the issues.	

6 Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 4 - Organizational Security Policies

	<u>, , , , , , , , , , , , , , , , , , , </u>
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.

7 Clarification of Scope

The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and misconfiguration. It provides a management interface to configure the system and generate reports regarding the results of the scans.

The TOE consists of the following components:

- Enterprise Manager Component The Enterprise Manager provides authorized users
 with access to the TOE through their Web browsers. It allows them to manage and
 run the TOE from anywhere on the network. Access is protected by user
 identification and authentication.
- 2. **Scan Engine Component** One or more Scan Engines scan the network environment. Depending on the logistics and size of your network, you may need more than one Scan Engine to scan the network. The Scan Engine performs identification, interrogation, and vulnerability assessment of remote computer systems.
- 3. **Scan Controller Component** The Scan Controller provides the communication between the scan engine and the database. Large or segmented networks (WANs) may require more than one scan controller to be deployed.
- API Service The API service provides an interface for Enterprise Manager to store data into and retrieve data from the Foundstone Database. This interaction uses SOAP over SSL.
- 5. **Data synchronization service** The Data Synchronization Service enables Vulnerability Manager to import asset information from McAfee's ePO enterprise management system or an LDAP directory such as Microsoft Active Directory. This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.
- 6. Foundstone Database The Foundstone Database is the data repository for the Vulnerability Manager system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and Scan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.
- 7. **Report Server** The Report Server is responsible for generating reports requested by authorized users. It retrieves scan results from the Foundstone Database, prepares the report, and saves it for future review.
- 8. **Web Application Scanner** The Web Application Scanner provides a scan configuration, vulnerability checks, and scan reports for web applications. The web application scanner module is a licensed item which can be purchased and added on to a Vulnerability Manager v7.0 deployment at any time. Any scan engine is capable of web application scanning once the module has been purchased with no additional software required.

In the evaluated configuration, the TOE is configured to disable the Foundstone Update capability. In addition, the following items are excluded from the evaluation:

- 1. Remediation management and tickets this is optional functionality requiring the purchase of an additional license. Not evaluated in the evaluated configuration.
- 2. Notification service this is optional functionality requiring the purchase of an additional license. Not evaluated in the evaluated configuration.

8 Architecture Information

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the Enterprise Manager software is installed must be dedicated to functioning as the Enterprise Manager. The TOE requires the following hardware and software configuration on this platform.

Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
2 GB RAM
Disk Space 80GB Partition
Windows Server 2003 SP2 or later
Windows Server 2008 R2
Current security updates
Internet Information Services (IIS) 6.0 or 7.5 if using Windows 2008 R2
Current IIS security patches
World Wide Web Publishing must be running

The platform on which the Scan Engine software is installed must be dedicated to functioning as a Scan Engine, with the exception of the Primary Scan Engine also providing the API Service and Data Sync Service. The TOE requires the following hardware and software configuration on this platform.

Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better 2 GB RAM
Disk Space 80GB Partition
Windows Server 2003 SP2 or later
Windows Server 2008 R2
Current security updates
MDAC 2.8
SQL Client Tools
Microsoft Windows Script 5.6

The platform on which the Foundstone Database and Report Server are installed must be dedicated to functioning as the servers for these functions of the TOE. The DBMS is installed on this same platform. The TOE requires the following hardware and software configuration on this platform.

Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better Disk Space D2 GB RAM 80GB Partition Windows Server 2003 SP2 or later Windows Server 2008 R2 Current security updates Microsoft SQL Server 2005 SP2 or later Microsoft SQL Server 2008 SP1 or later Microsoft SQL Express 2008 SP1 or later

All SQL hotfixes/patches SQL Server Memory Settings 900MB

Authorized users can access the Enterprise Manager through their Web browser software. The TOE supports Microsoft Internet Explorer 6.0 and higher, running on a Windows operating system. Latest service packs should be applied to both your browser and operating system. The security updates in Microsoft Knowledge Base MS06-013 must be applied to the client browser. Recommended minimum screen resolution is 1024 x 768.

9 Product Delivery

Software Delivery Description

McAfee software products are delivered to customers through an electronic download process. Once the purchase of a software product has been processed through the McAfee order fulfillment system, a Grant Code and download instructions are sent to the customer via email. A URL hyperlink to the download server is communicated to the customer as part of the download instructions. The Grant Code provides access (for up to one month) to the relevant downloadable files on a McAfee download server. The final release version of the product is tested, authorized for release, and posted to a McAfee download server. Multiple versions of the product may be available on the server. The customer shall download the Common Criteria certified version (as specified in the TOE Security Target) and documentation from the McAfee download server. The documentation package includes installation and supplemental configuration instructions.

Software Delivery Security Mechanisms General Security Mechanisms

All software released to customers are developed by McAfee software engineers and tested by a dedicated Quality Assurance (QA) organization. When QA considers a release candidate package to be ready for customer release, the results of QA testing are presented to a Management Team for a final authorization to release to web (RTW). If the Management Team gives approval to release the final release candidate package, QA uploads the final product (software and documentation) to the McAfee download server. QA posts the final, validated files on an internal secured server where the files are scanned for malware and stored. Access controls to this sever are management by McAfee Information Technology group and audited by McAfee Risk Management. QA verifies the integrity of the package prior to posting. QA then uses a proprietary Posting Tool to post the product and documentation files from the internal secured server onto the McAfee download server. The download server is accessible from the Internet by customers who have been explicitly granted access via the Grant Code process. Each Grant Code is unique and only provides access to the products the customer is entitled to. Checksums are saved for all files posted to the download server so that unauthorized modifications may be detected. After posting new files, QA performs a test download and verifies that the checksums are correct.

Download Security Mechanisms

As described above, Grant Codes are unique per customer and provide access to the software the customer has purchased. Grant Codes are sent directly to the named contact on the customer's order and are valid for 30 days before they expire. The McAfee download server uses HTTPS (or SSL encryption) to secure the link between the customer and the download server. After entering the appropriate Grant Code, the customer is presented with a page permitting them to select the available versions of the product they are entitled to download. The customer shall select the appropriate product version (as specified in the TOE Security Target) and associated documentation to download the Common Criteria evaluated product. The McAfee download server is located at a secure corporate data center behind a series of firewalls within a controlled and monitored DMZ. Download files may only be placed onto the

download server by authorized users located within the McAfee corporate intranet. The ability to upload and update the files on the download server is restricted to authorized personal with valid credentials and is subject to explicit approval by management.

Selecting the "Documentation" tab at the website download page permits the administrator to download the following documents.

- A) MVM7.0_DocSet_1.zip
- B) MVM700 Best Practices Guide.pdf
- C) MVM700 enabling localized reporting.pdf
- D) mvm700 epo40 product guide1.pdf
- E) MVM700_epo450_epo460_product_guide.pdf
- F) MVM700_FDCC_Benchmark_Scans.pdf
- G) MVM700_Hardening_Wizard_TechNote.pdf
- H) MVM700_Install_guide_1.pdf
- I) MVM700_PA520_Integration_Guide.pdf
- J) MVM700_Product_guide_1.pdf
- K) MVM700_Readme.html
- L) MVM700_Technote_System_Requirements_1.pdf
- M) MVM700_Virtualization.pdf
- N) MVM701_Quarterly_Technote.pdf
- O) MVM702_Quarterly_Technote1.pdf
- P) Readme_epo460.html

Not all of the documentation listed above is applicable the McAfee Vulnerability Manager 7.0 when it is placed into the Common Criteria evaluated configuration.

The following documents are applicable to the Common Criteria evaluated configuration. These documents were downloaded and evaluated.

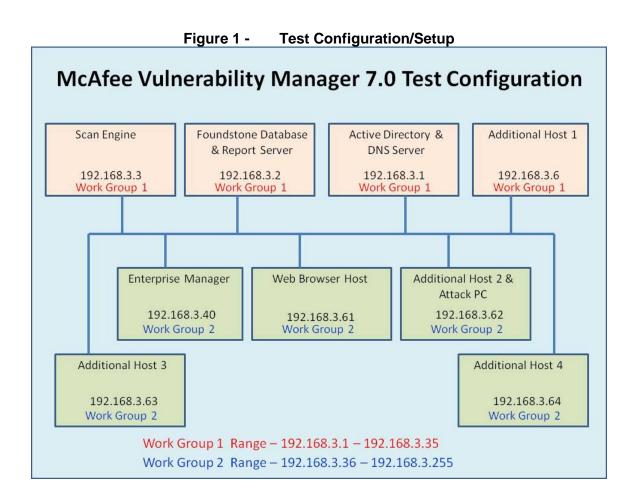
- A) Best Practices Guide McAfee Vulnerability Manager, October 4, 2010
- B) Installation Guide McAfee Vulnerability Manager, July 23, 2010
- C) Product Guide McAfee Vulnerability Manager 7.0, July 23, 2010
- D) Release Notes for McAfee Vulnerability Manager 7.0.0
- E) MVM700 Technote System Requirements.pdf

10 IT Product Testing

Testing was completed on October 3, 2011 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

10.1 Evaluator Functional Test Environment

Testing was performed on the following test bed configuration.



An overview of the purpose of each of these systems is provided in the following table.

Table 5 - Test Configuration Overview

System	Purpose
Enterprise Manager	This system provides the Enterprise Manager functionality for the testing.
Scan Engine	This system provides the Scan Engine functionality for the testing. Only one scan engine is used in the

System	Purpose
	testing. The API Service and Data Sync Service are also installed on this platform.
Foundstone Database and Report Server	This system provides the Foundstone Database and report generation functionality for the testing. The DBMS also executes on this platform.
Web Browser Host	This system provides a web browser for accessing the Enterprise Manager.
Active Directory & DNS Server	This system provides the Active Directory and Domain Name System (DNS) infrastructure for the testing.
Additional Host & Attack PC	This is an additional host that will be part of the scanned Work Group 2. This system will also be configured to be used as the Attack PC used for penetration testing.
Additional Host	This is an additional host that will be part of the scanned Work Group 1.
Switch	Not shown in the figure above, but included in the test configuration is a NetGear GS716T switch that will be used to connect the different systems on the network.

Specific configuration details for each of the systems are provided in the tables below.

Table 6 - Enterprise Manager Minimum Requirements

	Enterprise Manager Minimum Requirements
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating	Windows Server 2008 R2 (Including all updates and patches)
System	Current security updates.
Additional	Internet Information Services (IIS) 7.5
Software	Current IIS security patches
	World Wide Web Publishing must be running
	WireShark 1.0.2
	Snaglt Adobe Reader
Network Card	Ethernet

Disk Partition Formats	NTFS
Configuration	Static IP address 192.168.3.40
	FQDN: EM.CoactLab.local

Table 7 - Foundstone Database & Report Server Minimum Requirements

Foundstone Database & Report Server Minimum Requirements	
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows Server 2008 R2 (Including all updates and patches)
Additional	Microsoft SQL Server 2005 SP2
Software	All SQL hotfixes/patches
	All .NET hotfixes and patches
	WireShark 1.0.2
	Snaglt 8
Network Card	Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
SQL Server Memory Settings	900MB
Required Services	n/a
Configuration	Static IP address 192.168.3.2
	FQDN: FDB_RS.CoactLab.local

Table 8 - Scan Engine Details

Item	Purpose
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating	Windows Server 2008 R2 (Including all updates and patches)
System	Current security updates.

Item	Purpose
Additional	SQL Client Tools
Software	WireShark 1.0.2
	Snaglt 8
Network Card	Ethernet
Virtual Memory	2.0 GB
Disk Partition	NTFS
Formats	
Required	NetBIOS over TCP/IP
Services	
Configuration	Static IP address 192.168.3.3
	FQDN: SE.CoactLab.local

Table 9 - Web Browser Host Details

Item	Purpose
Hardware	Processor: 1 GHz Pentium 4
	Memory: 1 GB
	Disk Space: 8 GB
Installed software	Windows XP Professional SP3 (Including all updates and patches)
	Internet Explorer (Including all updates and patches)
	Snaglt 8
	WireShark 1.0.2
	Adobe Reader
Configuration	Static IP address 192.168.3.61
	FQDN: WBHost.CoactLab.local

Table 10 - Additional Host 2 & Attack PC Details

Item	Purpose
Installed software	Windows XP Professional SP3 (Including all updates and patches) Internet Explorer (Including all updates and patches) WinZip 10 ZENMAP GUI 5.21 Nmap 5.21
	NEWT 3 Snaglt 8 WireShark 1.0.2 Nessus Version 4.2 Paros Proxy 3.2.13
Configuration	Static IP address 192.168.3.62 FQDN: Attack.CoactLab.local

Table 11 - Active Directory & DNS Server Details

Item	Purpose
Installed	Microsoft Windows 2003 Server R2 (Including all updates and
software	patches)
Configuration	Static IP address 192.168.3.1
	FQDN: AD-DNS.CoactLab.local
	Primary Domain Controller for CoactLab.local

Table 12 - Additional Host 1 PC Details

Item	Purpose
Installed software	Windows XP SP1 (NO Service Pack Updates) Internet Explorer 6.0 (NO Service Pack Updates) WireShark 1.0.8 Snag It 8
Configuration	Static IP address 192.168.3.6 FQDN: AddHost.CoactLab.local

Table 13 - Additional 3 Host PC Details

Item	Purpose
Installed software	Power MAC G5 OS 10.4.11
Configuration	Static IP address 192.168.3.63 FQDN: AddHost3.CoactLab.local

Table 14 - Additional 4 Host PC Details

Item	Purpose
Installed software	Linux Red Hat 5.1
Configuration	Static IP address 192.168.3.64 FQDN: AddHost4.CoactLab.local

10.2 Functional Test Results

The repeated developer test suite includes all of the developer functional tests. Additionally, each of the Security Function and developer tested TSFI are included in the CCTL test suite. Results are found in the E2-0511-023(5) McAfee Vulnerability Manager 7.0 Evaluation Test Report dated October 21, 2011.

10.3 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

10.4 Evaluator Penetration Tests

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- A) http://osvdb.org/
- B) http://secunia.com/
- C) http://web.nvd.nist.gov
- D) http://securityfocus.com

The evaluator performed the public domain vulnerability searches using the following key words.

- A) McAfee
- B) McAfee 7.0
- C) McAfee Vulnerability
- D) Vulnerability Manager
- E) McAfee Manager
- F) Web Scanner

The evaluator selected the search key words based upon the following criteria.

- A) The searches that contained the keywords "McAfee" were selected to further refine the search directly related to the TOE.
- B) The product numbers were selected to determine if any identified vulnerability that was identified was applicable to the TOE.

The evaluator performed the public domain vulnerability searches for the following required third party products.

- A) MDAC 2.8
- B) SQL Client Tools
- C) Microsoft Windows Script 5.6
- D) IIS 6.0
- E) Microsoft SQL Server 2005

These keywords were chosen to identify the third party products and then narrow it down to the specific product version number.

The evaluator searched other developers for products and compared the products to the TOE. The evaluator identified the IBM/ISS Proventia Network Enterprise Scanner as a comparable technology type product. Vulnerabilities associated with the Proventia Network Enterprise Scanner were analyzed to determine if these vulnerabilities could be related to the TOE and identified as a potential vulnerability. The keywords used for this search included the following:

- A) Proventia
- B) Network Enterprise Scanner

This search was conducted in order to search other developer products and determine if any "technology type" product vulnerabilities could be relevant to this TOE type. These products are specified at their respective product websites.

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. No specific vulnerabilities were identified that could be associated directly with the TOE. Vulnerability searches were conducted on "technology type" related products. No vulnerabilities were identified that could be associated with the McAfee Vulnerability Manager.

11 Validator Comments

The validators' comments have been captured above in Section 7: Clarification of Scope.

12 Security Target

McAfee Corporation's Vulnerability Manager Version 7.0 Security Target Version 0.8, October 21, 2011

13 List of Acronyms AD Active Directory ADO ActiveX Data Objects CCE Common Configuration Enumeration CPE Common Platform Enumeration CVE Common Vulnerabilities and Exposures DBMS DataBase Management System EAL Evaluation Assurance Level ePO ePolicy Orchestrator FDCC Federal Desktop Core Configuration GUI Graphical User Interface ICMP Internet Control Message Protocol IP Internet Protocol IPS Intrusion Prevention System IT Information Technology LDAP Lightweight Directory Access Protocol MAC Media Access Control MDAC Microsoft Data Access Components NTFS New Technology File System NTLM...... NT LAN Manager OS Operating System OVAL Open Vulnerability Assessment Language PP Protection Profile SCAP Security Content Automation Protocol SF Security Function SOAPSimple Object Access Protocol SP Service Pack SQLStructured Query Language SSL Secure Socket Layer ST Security Target TCPTransmission Control Protocol TOE Target of Evaluation TSFI TSF Interface UDP User Datagram Protocol XCCDFeXtensible Configuration Checklist Description Format

14 Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 3.1, Revision 3, dated July 2009
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, dated July 2009
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000