Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee Corporation’s
Vulnerability Manager Version 6.8

Report Number: CCEVS-VR-VID10322-2011
Dated: 31 January 2011
ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
James Brosey

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587
McAfee Corporation’s  
Vulnerability Manager Version 6.8 Validation Report

Table of Contents

1 Executive Summary .................................................. 5
2 Identification ............................................................ 7
2.1 Applicable Interpretations ......................................... 8
3 TOE Description ....................................................... 8
4 Assumptions ............................................................. 9
5 Threats ................................................................... 10
6 Security Policies ......................................................... 11
7 Clarification of Scope .................................................. 11
8 Architecture Information ............................................. 13
9 Product Delivery ......................................................... 14
10 IT Product Testing ....................................................... 17
10.1 Evaluator Functional Test Environment ....................... 17
10.2 Functional Test Results ............................................. 22
10.3 Evaluator Independent Testing .................................. 22
10.4 Evaluator Penetration Tests ..................................... 22
11 VALIDATOR COMMENTS ........................................... 24
12 Security Target ......................................................... 25
13 List of Acronyms ....................................................... 25
14 Bibliography ........................................................... 26
McAfee Corporation’s
Vulnerability Manager Version 6.8 Validation Report

List of Figures
Figure 1 - Test Configuration/Setup .......................................................... 17

List of Tables
Table 1 - Evaluation Identifier ........................................................................ 7
Table 2 - Assumptions .................................................................................... 9
Table 3 - Threats ........................................................................................... 10
Table 4 - Organizational Security Policies ...................................................... 11
Table 5 - Test Configuration Overview .......................................................... 17
Table 6 - Enterprise Manager Details ............................................................ 18
Table 7 - Foundstone Database & Report Server Details .............................. 18
Table 8 - Scan Engine Details ........................................................................ 19
Table 9 - Web Browser Host Details .............................................................. 20
Table 10 - Additional Host & Attack PC Details ........................................... 20
Table 11 - Active Directory & DNS Server Details ....................................... 20
Table 12 - Additional 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 6.8 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 6 December 2010. 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 3, 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 6.8.

The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and mis-configurations. 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:

1. 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. 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. 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.

4. The Data Sync Service enables Vulnerability Manager to import asset information from McAfee’s ePolicy Orchestrator (ePO) enterprise management system or an LDAP directory such as Microsoft Active Directory. “The TOE may also be configured to import data about assets from external Data Sources, such as LDAP servers or ePO servers in the IT environment. Both LDAP and ePO databases contain detailed information about computer assets that may be of interest to administrators. This information may be imported from these Data Sources to be used by the TOE. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans. Note that the integration of the TOE with ePO is for data import only; ePO does not provide any management functionality of the TOE.” This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.

5. 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.

6. 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.

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>
<thead>
<tr>
<th>Table 1 - Evaluation Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Vulnerability Manager Version 6.8</td>
</tr>
<tr>
<td><strong>Evaluation Scheme</strong></td>
</tr>
<tr>
<td>TOE</td>
</tr>
<tr>
<td>Protection Profile</td>
</tr>
<tr>
<td>Conformance Result</td>
</tr>
<tr>
<td>Version of CC</td>
</tr>
<tr>
<td>Version of CEM</td>
</tr>
<tr>
<td>Sponsor</td>
</tr>
<tr>
<td>Developer</td>
</tr>
</tbody>
</table>
| Evaluator(s) | COACT Incorporated  
Bob Roland  
Greg Beaver  
Pascal Patin |
2.1 Applicable Interpretations
The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations
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 those assets. This solution allows managers to continuously monitor, respond to, 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>
<thead>
<tr>
<th>Assumption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.ACCESS</td>
<td>The TOE has access to all the IT System data it needs to perform its functions.</td>
</tr>
<tr>
<td>A.DYNNMIC</td>
<td>The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.</td>
</tr>
<tr>
<td>A.ASCOPE</td>
<td>The TOE is appropriately scalable to the IT System the TOE monitors.</td>
</tr>
<tr>
<td>A.PROTCT</td>
<td>The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.</td>
</tr>
<tr>
<td>A.LOCATE</td>
<td>The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.</td>
</tr>
<tr>
<td>A.MANAGE</td>
<td>There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.</td>
</tr>
<tr>
<td>A.NOEVIL</td>
<td>The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.</td>
</tr>
<tr>
<td>A.ALARM</td>
<td>The DBMS will generate an alarm if storage space in the database is exhausted.</td>
</tr>
<tr>
<td>A.DATABASE</td>
<td>Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>T.COMDIS</th>
<th>An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.LOSSOFF</td>
<td>An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.</td>
</tr>
<tr>
<td>T.COMINT</td>
<td>An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.</td>
</tr>
<tr>
<td>T.NOHALT</td>
<td>An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.</td>
</tr>
<tr>
<td>T.PRIVIL</td>
<td>An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.</td>
</tr>
<tr>
<td>T.IMPCON</td>
<td>An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.</td>
</tr>
<tr>
<td>T.SCNCFG</td>
<td>Improper security configuration settings may exist in the IT System the TOE monitors.</td>
</tr>
<tr>
<td>T.SCNMLC</td>
<td>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.</td>
</tr>
<tr>
<td>T.SCNVUL</td>
<td>Vulnerabilities may exist in the IT System the TOE monitors.</td>
</tr>
<tr>
<td>T.FALREC</td>
<td>The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source.</td>
</tr>
<tr>
<td>T.FALASC</td>
<td>The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources.</td>
</tr>
<tr>
<td>T.FACCNT</td>
<td>Unauthorized attempts to access TOE data or security functions may go undetected.</td>
</tr>
<tr>
<td>T.FALACT</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.DETECT</td>
<td>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.</td>
</tr>
<tr>
<td>P.ANALYZ</td>
<td>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.</td>
</tr>
<tr>
<td>P.MANAGE</td>
<td>The TOE shall only be managed by authorized users.</td>
</tr>
<tr>
<td>P.ACCESS</td>
<td>All data collected and produced by the TOE shall only be used for authorized purposes.</td>
</tr>
<tr>
<td>P.INTGTY</td>
<td>Data collected and produced by the TOE shall be protected from modification.</td>
</tr>
<tr>
<td>P.PROTCT</td>
<td>The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.</td>
</tr>
<tr>
<td>P.ACCACT</td>
<td>Users of the TOE shall be accountable for their actions within the TOE.</td>
</tr>
</tbody>
</table>

7 Clarification of Scope
The McAfee Vulnerability Manager Version 6.8 TOE components are described in the following sections:

The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and mis-configurations. 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:

1. 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. 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. 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.
4. The Data Sync Service enables Vulnerability Manager to import asset information from McAfee’s ePolicy Orchestrator (ePO) enterprise management system or an LDAP directory such as Microsoft Active Directory. The TOE may also be configured to import data about assets from external Data Sources, such as LDAP servers or ePO servers in the IT environment. Both LDAP and ePO databases contain detailed information about computer assets that may be of interest to administrators. This information may be imported from...
these Data Sources to be used by the TOE. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans. Note that the integration of the TOE with ePO is for data import only; ePO does not provide any management functionality of the TOE.” This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.

5. 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.

6. 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.

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.

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.

- Processor Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
- Memory 2 GB RAM
- Disk Space 80GB Partition
- Operating System Windows Server 2003 SP2 (minimum)
- Current security updates, including the JScript update provided in
- Microsoft Security Bulletin MS06-023
- Additional Software IIS 6.0
- Current IIS security patches
- World Wide Web Publishing must be running
- OpenSSL v1.2
- PHP v5.2.1
- Network Card Ethernet
- Disk Partition Formats NTFS

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.

- Processor Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
- Memory 2 GB RAM
- Disk Space 80GB Partition
- Operating System Windows Server 2003 SP2 (minimum)
- Current security updates, including the JScript update provided in
- Microsoft Security Bulletin MS06-023
- Additional Software MDAC 2.8
- SQL Client Tools (for Microsoft SQL Server 2005)
- OpenSSL v1.2
- PuTTY SSH Client v0.60jo
- Microsoft Windows Script 5.6
- Network Card Ethernet
- Virtual Memory 2.0 GB
- Disk Partition Formats NTFS
- Required Services NetBIOS over TCP/IP
- Print Spooler
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.

- Processor Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
- Memory 2 GB RAM
- Disk Space 80GB Partition
- Operating System Windows Server 2003 SP2 (minimum)
- Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
- Additional Software Microsoft SQL Server 2005 SP1 and all SQL hotfixes/patches
- Network Card Ethernet
- Virtual Memory 2.0 GB
- Disk Partition Formats NTFS
- SQL Server Memory
- Settings
- 900MB
- Required Services n/a

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 as shown in Figure 1. 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 server 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.

The following documents may be downloaded from the McAfee website:

A) McAfee Vulnerability Manager Configuration Manager, 9/18/2009, Foundstone Publication 700-27201--00 / Document Build 1.0
B) Foundstone 6.8 Database Maintenance Guide, 9/18/2009, 700-1625-00 / Document Build 1.0
D) 6.8 Enterprise Manager Administrator Guide, Issued 9/18/2009, Foundstone Publication 700-1618-00 / Document Build 1.0
The following documents may be downloaded from the McAfee website, but were not evaluated in the present evaluation:

A) McAfee Vulnerability Manager Configuration Manager, 9/18/2009, Foundstone Publication 700-27201--00 / Document Build 1.0

B) MVM_SCAP_Implementation.pdf
10 IT Product Testing

Testing was completed on November 30, 2010 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.

![Test Configuration/Setup](image)

**McAfee Vulnerability Manager 6.8 Test Configuration**

- **Scan Engine**: 192.168.3.3, **Work Group 1**
- **Foundstone Database & Report Server**: 192.168.3.2, **Work Group 1**
- **Active Directory & DNS Server**: 192.168.3.1, **Work Group 1**
- **Additional Host**: 192.168.3.6, **Work Group 1**

- **Enterprise Manager**: 192.168.3.40, **Work Group 2**
- **Web Browser Host**: 192.168.3.51, **Work Group 2**
- **Additional Host & Attack PC**: 192.168.3.62, **Work Group 2**

*Work Group 1 Range – 192.168.3.1 – 192.168.3.35
Work Group 2 Range – 192.168.3.36 – 192.168.3.255*

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

**Table 5 - Test Configuration Overview**

<table>
<thead>
<tr>
<th>System</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Manager</td>
<td>This system provides the Enterprise Manager functionality for the testing.</td>
</tr>
<tr>
<td>Scan Engine</td>
<td>This system provides the Scan Engine functionality for the testing. Only one scan engine is used in the testing. The API Service and Data Sync Service are also installed on this platform.</td>
</tr>
<tr>
<td>Foundstone Database and Report Server</td>
<td>This system provides the Foundstone Database and report generation functionality for the testing. The DBMS also executes</td>
</tr>
</tbody>
</table>
System | Purpose
--- | ---
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 Details**

<table>
<thead>
<tr>
<th>Enterprise Manager Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Pentium D 2.8G</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB RAM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>75GB Partition</td>
</tr>
</tbody>
</table>
| Operating System | Windows Server 2003 SP2  
Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023 |
| Additional Software | IIS 6.0  
Current IIS security patches  
World Wide Web Publishing  
OpenSSL v1.2  
PHP v5.2.1  
WireShark 1.0.2  
SnagIt 8 |
| Network Card | Ethernet |
| Disk Partition Formats | NTFS |
| Configuration | Static IP address 192.168.3.40  
FQDN: EM.CoactLab.com |

**Table 7 - Foundstone Database & Report Server Details**
## Foundstone Database & Report Server Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel P4 3.2 G</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB RAM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>40GB Partition</td>
</tr>
</tbody>
</table>
| Operating System      | Windows Server 2003 SP2  
Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023 |
| Additional Software   | Microsoft SQL Server 2005 SP2 and all SQL hotfixes/patches  
WireShark 1.0.2  
SnagIt 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.com                                                              |

## Table 8 - Scan Engine Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon 2.8Ghz</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB RAM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>38GB Partition</td>
</tr>
</tbody>
</table>
| Operating System      | Windows Server 2003 SP2  
Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023 |
| Additional Software   | MDAC 2.8  
SQL Client Tools (for Microsoft SQL Server 2005)  
OpenSSL v1.2  
PuTTY SSH Client v0.60jo  
Microsoft Windows Script 5.6  
WireShark 1.0.2  
SnagIt 8 |
<p>| Network Card          | Ethernet                                                                                                                                |
| Virtual Memory        | 2.0 GB                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Partition Formats</td>
<td>NTFS</td>
</tr>
<tr>
<td>Required Services</td>
<td>NetBIOS over TCP/IP</td>
</tr>
<tr>
<td>Configuration</td>
<td>Static IP address 192.168.3.3</td>
</tr>
<tr>
<td></td>
<td>FQDN: SE.CoactLab.com</td>
</tr>
</tbody>
</table>

**Table 9 - Web Browser Host Details**

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Processor: 1 GHz Pentium 4</td>
</tr>
<tr>
<td></td>
<td>Memory: 1 GB</td>
</tr>
<tr>
<td></td>
<td>Disk Space: 8 GB</td>
</tr>
<tr>
<td>Installed software</td>
<td>Windows XP Professional SP3</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 6.0 SP1 or later</td>
</tr>
<tr>
<td></td>
<td>SnagIt 8</td>
</tr>
<tr>
<td></td>
<td>WireShark 1.0.2</td>
</tr>
<tr>
<td>Configuration</td>
<td>Static IP address 192.168.3.61</td>
</tr>
<tr>
<td></td>
<td>FQDN: WBHost.CoactLab.com</td>
</tr>
</tbody>
</table>

**Table 10 - Additional Host & Attack PC Details**

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software</td>
<td>Windows XP Professional SP3</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 6.0 SP1 or later</td>
</tr>
<tr>
<td></td>
<td>WinZip 10</td>
</tr>
<tr>
<td></td>
<td>ZENMAP GUI 5.21</td>
</tr>
<tr>
<td></td>
<td>Nmap 5.21</td>
</tr>
<tr>
<td></td>
<td>NEWT 3</td>
</tr>
<tr>
<td></td>
<td>SnagIt 8</td>
</tr>
<tr>
<td></td>
<td>WireShark 1.0.2</td>
</tr>
<tr>
<td></td>
<td>Nessus Version 4.2</td>
</tr>
<tr>
<td></td>
<td>Paros Proxy 3.2.13</td>
</tr>
<tr>
<td>Configuration</td>
<td>Static IP address 192.168.3.62</td>
</tr>
<tr>
<td></td>
<td>FQDN: Attack.CoactLab.com</td>
</tr>
</tbody>
</table>

**Table 11 - Active Directory & DNS Server Details**

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software</td>
<td>Microsoft Windows 2000 Server SP4</td>
</tr>
<tr>
<td>Item</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration</td>
<td>Static IP address 10.1.13.254</td>
</tr>
<tr>
<td>FQDN: AD-DNS.CoactLab.com</td>
<td></td>
</tr>
<tr>
<td>Primary Domain Controller for CoactLab.com</td>
<td></td>
</tr>
</tbody>
</table>

### Table 12 - Additional Host PC Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software</td>
<td>Windows XP SP1</td>
</tr>
<tr>
<td></td>
<td>WireShark 1.0.8</td>
</tr>
<tr>
<td>Configuration</td>
<td>Static IP address 192.168.3.6</td>
</tr>
<tr>
<td>FQDN: AddHost.CoactLab.com</td>
<td></td>
</tr>
</tbody>
</table>
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 E2-0810-004(3) McAfee Vulnerability Manager 6.8 Evaluation Test Report, dated December 2, 2010.

Functionality Not Tested
The following SFR has not been tested:

IDS_STG.2.1 The System shall **ignore System data** if the storage capacity has been reached.

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 support the identification of possible potential vulnerabilities in the TOE. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below.

A) http://cve.mitre.org
B) http://google.com
C) http://osvdb.org/
D) http://www.securityfocus.com/
E) http://secunia.com/
F) http://www.us-cert.gov
G) http://securitytracker.com/
H) http://web.nvd.nist.gov
I) http://www.cvedetails.com/

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

A) McAfee
B) McAfee 6.8
C) McAfee Vulnerability
D) Vulnerability Manager
E) McAfee Manager
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) OpenSSL v1.2
B) PHP v5.2.1
C) IIS 6.0
D) MDAC 2.8
E) PuTTY SSH Client v0.60jo
F) Microsoft Windows Script 5.6
G) Microsoft SQL Server 2005 SP1

The evaluator used the following keywords to search for vulnerabilities for the required third party products.

A) OpenSSL v1.2
B) PHP v5.2.1
C) PHP 5.2.1
D) IIS 6.0
E) IIS
F) PuTTY SSH Client v0.60jo
G) PuTTY 0.60
H) Microsoft Windows Script 5.6
I) Windows Script 5.6
J) SQL Server 2005
K) SQL Server 2005 SP1

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
C) Vulnerability 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 evaluators conducted a search to verify if any obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

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

Remediation management and Notification Service are optional functionality, not included in the TOE, requiring the purchase of additional licenses. These functions are not included in the evaluated configuration.

Security functionality is stated in the TOE Summary Specification portion of the ST with no requirement to back it up. The ST claims that the TOE protects the password from visual detection by echoing back asterisks (“*”) for the entered passwords. This was functionality was not verified.

The Validator recommends that strong passwords be used and that passwords are changes often.
12 Security Target

McAfee Corporation’s Vulnerability Manager Version 6.8 Security Target, version 2.4, January 11, 2011.

13 List of Acronyms

AD ................................................................. Active Directory
ADO ........................................................................ ActiveX Data Objects
API ................................................................. Application Program Interface
CC ...................................................................... Common Criteria
CCE ................................................................. Common Configuration Enumeration
CM ................................................................. Configuration Management
CPE ..................................................................... Common Platform Enumeration
CVE ................................................................. Common Vulnerabilities and Exposures
CVSS ............................................................. Common Vulnerability Scoring System
DBMS ............................................................ DataBase Management System
DNS ................................................................. Domain Name System
EAL ................................................................. Evaluation Assurance Level
ePO ................................................................. ePolicy Orchestrator
FDCC ............................................................. Federal Desktop Core Configuration
GUI ....................................................................... Graphical User Interface
I&A ................................................................. Identification & Authentication
ICMP .............................................................. Internet Control Message Protocol
IDS ................................................................. Intrusion Detection System
IIS ................................................................. Internet Information Services
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
RAM ............................................................. Random Access Memory
SCAP ............................................................. Security Content Automation Protocol
SF ................................................................. Security Function
SFR ................................................................. Security Functional Requirement
SOAP ........................................................... Simple Object Access Protocol
SP ................................................................. Service Pack
SQL ............................................................... Structured Query Language
SSL ............................................................. Secure Socket Layer
ST ................................................................. Security Target
TCP ............................................................. Transmission Control Protocol
TOE ............................................................. Target of Evaluation
TSF ............................................................... TOE Security Function
14 Bibliography

The following list of standards was used in this evaluation:

- Guide for the Production of PPs and STs, Version 0.9, dated January 2000