Practical Audit of Antivirus software: How to Audit Norton 2005

GSNA

Practical Assignment

Version 3.2

Option 1

Amar I. Yousif
Auditing Networks, Perimeters, and Systems (GSNA)
SANS Houston, 2004

March 14, 2005

Abstract

In the age of information assurance, the technology audit is becoming more needed than ever before. We continue to depend increasingly on technology in medicine, critical infrastructure, corporate accounting, military operations, and a host of other areas. There is an undeniable need for reliable, repeatable, and mature processes to audit and certify the accuracy of the information being processed, transported, and stored with technology. An IT audit profession that is similar in many ways to the financial audit profession is inevitable.

In light of the above, the purpose of this paper is to explore the audit process by developing an audit program for auditing a certain technology, Norton Antivirus running on a windows XP home edition Operating System. The audience for this paper is auditors who are semi-expert in the subject matter. The audience should be able to conduct a full audit by following the procedures and guidelines in the paper.

Table of contents

Abstract 2

Table of contents 3

Introduction: 4

The Problem: 4

The Solution: 4

Part 1: The Research 5

The subject of the Audit 5

Identification of the risks 5

Current state of the practice 7

Part 2: The Audit Program 9

The Audit checklist 9

Practical Audit checklist for Norton 2005 10

Part 3: The Audit 22

Conducting the Audit 22

Sample Audit results 22

Part 4: The Audit Report 27

Executive summery 27

Audit findings 28

Audit recommendations 30

References 31

Introduction:

This paper is submitted to fulfill the requirements for the GSNA certification (practical assignment). The subject of the paper revolves around the IT audit practice. Simply put, I will attempt, through this paper, to develop an audit plan for a certain technology; namely Norton Anti-virus 2005.

The Problem:

Although the technology audit process, on a high level, is well defined by the industry and is well understood by auditors, the detailed technical procedures of auditing the numerous and ever-emerging technologies remains a challenge. A lack of expert knowledge in a certain system is a hindrance to the audit process conducted by a semi-expert auditor. Training all auditors to achieve expert level on all technologies is unfeasible to audit firms. There is a need for audit programs, AKA audit plans that are designed by expert auditors and can be followed systematically by other auditors. This will allow semi-expert auditors to conduct audits with the same quality results of audits conducted by expert-auditors. In this paper, I have elected Norton Anti-virus 2005 as the subject of the audit.

The Solution:

The purpose of this paper is to demonstrate the creation of an audit program by an expert auditor. This will serve two benefits:

1. Demonstrating, by example, the methodology with which an expert auditor creates an audit program to be used by semi-expert auditors.
2. As a final product, the paper will serve as a complete audit program for auditing an Anti-virus software; Norton 2005, running on a Windows operating system; Windows XP Home edition.

Part 1: The Research

The subject of the Audit

In today's highly interconnected computing environment, cyber threats are more than common. Viruses, Worms, and Trojans are various forms of malicious programs that could compromise a personal computer causing disclosure of critical information, decreased performance, or both. Antivirus software is designed to protect against those malicious programs. However, not all Antivirus implementations are created equal. The level of protection against malicious programs depends on a host of factors that are either configurable by the user or designed by the manufacturer of the Antivirus software. The purpose of this paper is to design an Audit program, AKA Audit plan, to test and verify the effectiveness of a certain Antivirus software, Norton 2005, running on a Windows XP home edition operating system.

Identification of the risks

Asset, Threat, and Vulnerability are identified as the triple of risk management (Krutz & Vines, 2003, p.18). When applied to the subject of the audit:

The Asset: The information stored on a PC and the performance level of that PC. In the case of a personal computer, this information includes; credit card information, cached passwords, personal data, usage history, etc.

The Threat: Malicious programs that could compromise the confidentiality, integrity, or availability of the information stored on a PC.

The Vulnerability: The lack of a safeguard against the threat; the vulnerability may be exploited by malicious programs.

In addition to the above, the industry defines risk as the probability that a threat will materialize causing harm to the assets. To mitigate the risk in our case, a safeguard, Antivirus software, is needed to reduce the system vulnerability to the threat; malicious programs.

Malicious programs come in different shapes and they continue to evolve into codes that are more dangerous. Below are a few examples of such programs as listed by Skoudis and Zeltser in their 2004 book titled (Malware: Fighting Malicious Code):

- Virus: Infects a host file (e.g., executable, word processing document, etc.). It self replicates and usually requires human interaction to do so (by opening a file, reading an e-mail, booting a system, or executing an infected program). Significant examples include; Michelangelo and CIH.
- Worms: Spread across a network. It self replicates and usually does not require human interaction to spread. Significant examples include; Morris Worm, Code Red, and SQL Slammer.
- Malicious Mobile Code: Consists of lightweight programs that are downloaded from a remote system and executed locally with minimal or no user intervention. It is typically written in Javascript, VBScript, Java, or ActiveX. Significant examples include; Cross Site Scripting.
- Backdoor: Bypasses normal security control to give an attacker access. Significant examples include; Netcat and Virtual Network Computing (VNC): Both can be used legitimately as remote administration tools, or illegitimately as attack tools.
- Trojan horse: Disguises itself as a useful program while masking hidden malicious purpose. Significant examples include; Setiri and Hydan.
- User-level RootKit: Replaces or modifies executable programs used by system administrators and users. Significant examples include; Linux RootKit (LRK) family, Universal RootKit, and FakeGINA.
- Kernel-level RootKit: Manipulates the heart of the operating system, the kernel, to hide and create backdoors. Significant examples include; Adore and Kernel Intrusion System.
- Combination malware: Combines various techniques already described to increase effectiveness. Significant examples include; Lion and Bugbear.B.

(Skoudis & Zeltser, 2004)

All of the above threats constitute a risk that could negatively affect confidentiality, integrity, and availability of the information stored on a vulnerable PC. A proper implementation of Antivirus software can effectively reduce that risk by reducing the level of the PC's vulnerability to the above-mentioned threats.

Current state of the practice

During the course of my research, I came across several organizations that provide independent Antivirus software testing and publish the results to the public. They run rigorous Antivirus tests against updated in-the-wild virus' lists to examine the effectiveness of Antivirus products. In-the-wild viruses are viruses that are still circulating in production environments as opposed to zoo viruses that are no longer in the wild and are contained in laboratories only. Researching the databases of Antivirus testing organizations is a good start to check the credibility of any commercial Antivirus software.

NIST:
The Computer Security Research Center of the National Institute of Standards and Technology (NIST) provides an excellent document in its archive with respect to the Antivirus software testing (Gordon & Howard, 2000).
http://csrc.nist.gov/nissc/2000/proceedings/papers/038.pdf

ICSA Labs:
The International Computer Security Association (ICSA) provides a monthly report of all Antivirus products they test.
http://www.icsalabs.com/html/communities/antivirus/labs.shtml#2005

Virus Bulletin:
The Virus Bulletin provides a continually updated list of tested Antivirus products.
http://www.virusbtn.com/vb100/archives/products.xml?table

West Coast Labs:
West coast labs provide checkmark level1, level2, and Trojan testing for many commercial Antivirus products.
http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=1

There is also a wealth of resources on the Internet delineating industry best practices for implementing and configuring Antivirus software.

Cert Coordination Center:
Cert coordination center operated by the Carnegie Mellon University provides home users with a security checklist that includes Antivirus software items.
http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist1.pdf

WEBtech:
WEBtech is an Internet presence provider. They provide a virus defence checklist.
http://www.webtech.on.ca/webtechantiviruschecklist.pdf

EnterpriseIT:
EnterpriseIT is an IT management solutions provider that provides an Antivirus protection checklist on their website.
http://www.enterprise-itm.com/AVChecklist.htm

PC Pitstop:
PC Pitstop, a PC auto-diagnostic and auto-detecting technologies provider, provides a five step guide to protect your PC.
http://www.pcpitstop.com/antivirus/AVirusNotes.asp

EICAR:
European **I**nstitute for **C**omputer **A**ntivirus **R**esearch (Eicar) provides standard Antivirus test files. The test files, although non-viral, act like a virus causing Antivirus software to identify them as viruses. These files are helpful when giving your Antivirus product a real life test.
http://www.eicar.org/anti_virus_test_file.htm

PC World:
Stan Miastkowski provides a comprehensive step-by-step guide on how set Antivirus software for maximum protection. His article was published in the January 2003 issue of the PC World magazine.
http://www.pcworld.com/howto/article/0,aid,106718,00.asp

In addition to the above, the SANS institute provides clear guidelines on how to design audit programs and how to conduct audits. Materials from www.SANS.org coupled with SANS training books for the GSNA track provide a wealth of information and examples on how to design and conduct technology audits.

Part 2: The Audit Program

The Audit checklist

The Audit program is as good as its respective Audit checklist. As defined by the SANS institute, each item in the Audit checklist must include the following:

- Checklist item number: Used for cross-referencing in the Audit conclusion.
- Checklist item title: A brief description of the item.
- Reference: Creditable reference that is the source or the inspiration behind the checklist item.
- Risk: The risk to the audited system.
- Testing procedures: Detailed procedures written for semi-expert auditors to follow when conducting the audit.
- Test nature: Subjective or Objective.
- Evidence: A place-marker for evidence that is generated by the testing procedures.
- Findings: A place-marker for the auditor’s findings.

Practical Audit checklist for Norton 2005

Item number	AV01
Title	Research third party testing results of the Antivirus software
References	ICSA Labs Virus Bulletin West Coast Labs
Risk	Failing a third party test against in-the-wild virus list means that the Antivirus detection and prevention controls can be circumvented by certain in-the-wild viruses
Testing procedures and compliance criteria	Search the below third party databases for the Antivirus software testing results. ICSA Labs http://www.icsalabs.com/html/communities/antivirus/labs.shtml#2005 Virus Bulletin http://www.virusbtn.com/vb100/archives/products.xml?table West Coast Labs http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=1 1. A failed test on any of the databases will constitute a fail on the audit item. 2. Only when point#1 is not true, then a passed test on any of the databases will constitute a pass on the audit item. 3. A no-test-results-found on all three of the databases will void the audit item.
Test nature	Objective
Evidence	
Findings	

Item number	AV02
Title	Verify that the virus definition file is updated automatically on regular basis; at least once a week.
References	WEBtech http://www.webtech.on.ca/webtechantiviruschecklist.pdf PC Pitstop http://www.pcpitstop.com/antivirus/AVirusNotes.asp
Risk	New virus signatures are not added to the definition file, which in its turn will cause the Antivirus software to let pass new viruses.
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Check the status of the Automatic LiveUpdate feature (It should be set to On). 2. Check the date of the Virus Definitions (It should not be older than one week).
Test nature	Objective
Evidence	
Findings	

Item number	AV03
Title	Verify that the Antivirus software is configured to scan all Internet downloads
Reference	EnterpriseIT http://www.enterprise-itm.com/AVChecklist.htm
Risk	Antivirus software not detecting malicious codes downloaded from the Internet.
Testing procedures and compliance criteria	1. Connect to the Internet. 2. Go to http://www.eicar.org/anti_virus_test_file.htm . 3. Right click on the Anti-Virus test file "eicar.com.txt" and choose (save as) to try downloading it to the desktop. 4. The Antivirus software should detect the test file as a virus.
Test nature	Objective
Evidence	
Findings	

Item number	AV04
Title	Verify that the Antivirus software is configured to scan all e-mails and e-mail attachments
References	Cert Coordination Center http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist1.pdf EnterpriseIT http://www.enterprise-itm.com/AVChecklist.htm
Risk	Antivirus software not detecting harmful malicious codes embedded in e-mails or included as attachments to e-mails.
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the options button. 2. Under the Internet menu, choose the E-mail button. You will be presented with the E-mail scanning screen. 3. Under (What to scan) look for the scan incoming e-mail and the scan outgoing e-mail check boxes; they both should be checked.
Test nature	Objective
Evidence	
Findings	

Item number	AV05
Title	Verify that the Antivirus software is configured to scan all file types.
References	EnterpriseIT http://www.enterprise-itm.com/AVChecklist.htm PC World Magazine (Article by Stan Miastkowski) http://www.pcworld.com/howto/article/0,aid,106718,pg,3,00.asp
Risk	Antivirus not scanning infected certain file types
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the Options button; you will be presented with the Auto-Protect screen. 2. The following options should be checked: a. Comprehensive file scanning. b. Scan within compressed files.
Test nature	Objective
Evidence	
Findings	

Item number	AV06
Title	Verify that Antivirus can detect malicious codes in compressed files.
Reference	**E**uropean **I**nstitute for **C**omputer **A**ntivirus **R**esearch (EICAR) http://www.eicar.org/anti_virus_test_file.htm
Risk	Not detecting viruses that are hidden inside a compressed file.
Testing procedures and compliance criteria	1. Connect to the Internet. 2. Go to http://www.eicar.org/anti_virus_test_file.htm . 3. Right click on the Anti-Virus test file “eicar_com.zip” and choose (save as) to try downloading it to the desktop. 4. The Antivirus software should detect the compressed test file as a virus.
Test nature	Objective
Evidence	
Findings	

Item number	AV07
Title	Verify that the Antivirus software is configured to perform a full system scan at least once a week
References	WEBtech http://www.webtech.on.ca/webtechantiviruschecklist.pdf PC Pitstop http://www.pcpitstop.com/antivirus/AVirusNotes.asp PC World Magazine (Article by Stan Miastkowski) http://www.pcworld.com/howto/article/0,aid,106718,pg,7,00.asp
Risk	Antivirus software not detecting doormat malicious code residing on the computer
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Check the Full System Scan date. It should not be older than one week. 2. Choose the Scan for Viruses tab. 3. Click on the schedule icon corresponding to the (Scan my computer) item. You will be presented with the schedule screen. 4. The scan should be scheduled to occur at least once a week.
Test nature	Objective
Evidence	
Findings	

Item number	AV08
Title	Verify that the Antivirus software checks every file as it is accessed
Reference	WEBtech http://www.webtech.on.ca/webtechantiviruschecklist.pdf
Risk	Antivirus software not detecting viruses on removable media (CDs, floppy disks, memory sticks, etc.)
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the Options button; you will be presented with the Auto-Protect screen. 2. The Enable Auto-Protect option should be checked.
Test nature	Objective
Evidence	
Findings	

Item number	AV09
Title	Verify that the heuristic virus checking is enabled
References	Cert Coordination Center http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist1.pdf PC World Magazine (Article by Stan Miastkowski) http://www.pcworld.com/howto/article/0,aid,106718,pg,5,00.asp
Risk	New viruses and variants of old viruses that could bypass the virus definition check will not be detected when the Antivirus heuristic checking is disabled.
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the Options button; you will be presented with the Auto-Protect screen. 2. On the left hand side, under System, click on the Auto-Protect option to collapse the menu. 3. Click on Bloodhound. You will be presented with the Bloodhound screen. 4. The (Enable Bloodhound heuristic) option should be checked.
Test nature	Objective
Evidence	
Findings	

Item number	AV10
Title	Verify that the Antivirus software is configured to automatically repair infected files.
Reference	PC World Magazine (Article by Stan Miastkowski) http://www.pcworld.com/howto/article/0,aid,106718,pg,6,00.asp
Risk	Incorrect choices by non-expert users when presented with an infected file
Testing procedures and compliance criteria	From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the Options button; you will be presented with the Auto-Protect screen. 2. The Automatically repair the infected file option should be checked.
Test nature	Objective
Evidence	
Findings	

Item number	AV11
Title	Verify that the instant messenger protection, a special feature of NAV2005, is enabled.
Reference	PC World Magazine (Article by Stan Miastkowski) http://www.pcworld.com/howto/article/0,aid,106718,pg,8,00.asp
Risk	Antivirus not detecting malicious codes transmitted through the use of instant messenger software
Testing procedures and compliance criteria	From your Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 1. Choose the Options button 2. On the left hand side, under Internet, click on the Instant Messenger option. You will be presented with the Instant Messenger screen. 3. Under (Which instant messengers to protect), all applicable options should be checked.
Test nature	Objective
Evidence	
Findings	

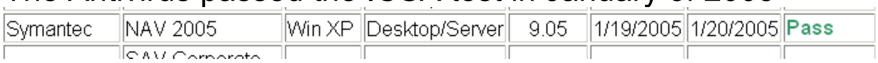
Item number	AV12
Title	Verify that the Antivirus software is configured to be automatically enabled upon PC startup
Reference	Personal experience
Risk	Antivirus protection is disabled after reboot giving the user a false sense of security
Testing procedure	1. Reboot the computer. 2. Logon to the computer. 3. From the Windows XP start menu, choose programs, Norton Antivirus, and then Norton Antivirus 2005. You will be presented with the System Status screen. 4. Under (security scanning features), the Auto-Protect should be (On).
Test nature	Objective
Evidence	
Findings	

Part 3: The Audit

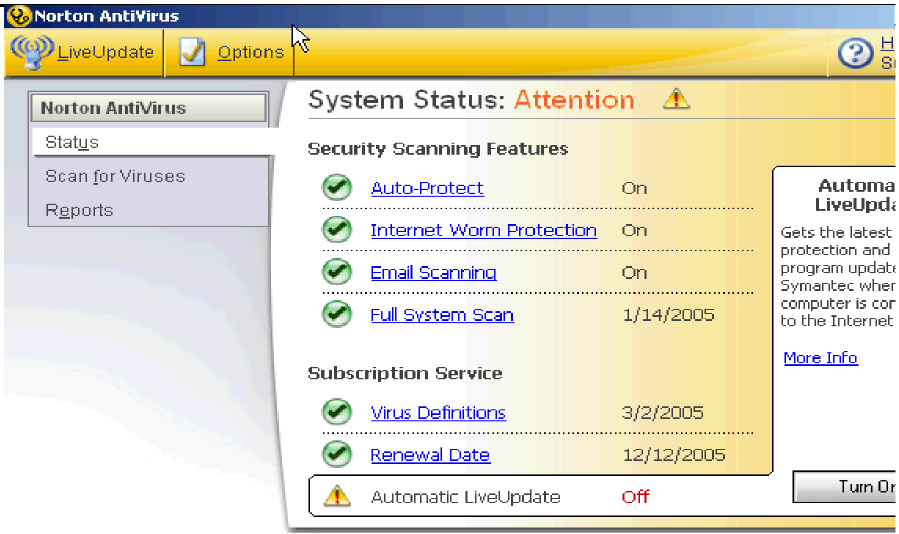
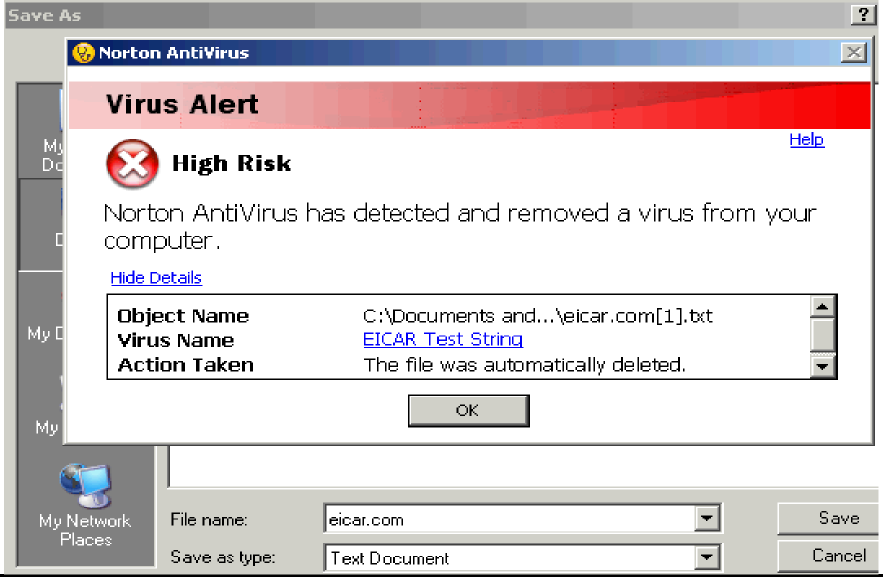
Conducting the Audit

The Audit checklist is the blueprint for the practical Audit. A well-developed Audit checklist enables the Auditor to examine thoroughly the system, gathering the needed evidence for the final report in the process. In the following section if this paper, we will choose ten Audit items from our previously developed checklist and conduct a practical Audit listing the findings and the evidence upon which we based our findings.

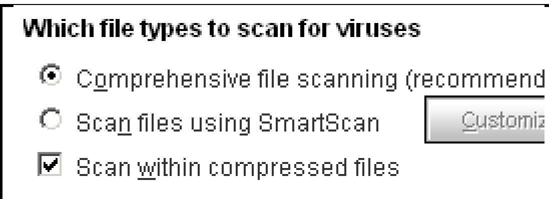
Sample Audit results

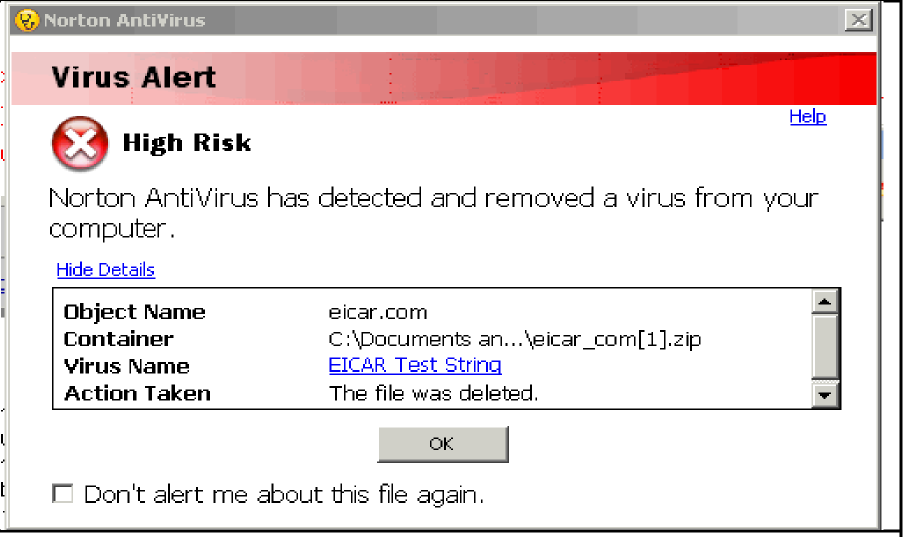
Item number	AV01
Title	Research third party testing results of the Antivirus software
Evidence	No Norton Antivirus 2005 failed test was found on all three databases The Antivirus passed the ICSA test in January of 2005  Symantec NAV 2005 Win XP Desktop/Server 9.05 1/19/2005 1/20/2005 Pass SAV Corporate
Findings	PASS

Item number	AV02
Title	Verify that the virus definition file is updated automatically on regular basis; at least once a week.

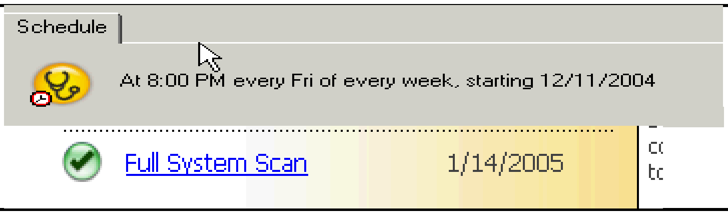
Evidence	 Norton AntiVirus LiveUpdate · Options Norton AntiVirus · Status · Scan for Viruses · Reports System Status: Attention Security Scanning Features Auto-Protect On Internet Worm Protection On Email Scanning On Full System Scan 1/14/2005 Subscription Service Virus Definitions 3/2/2005 Renewal Date 12/12/2005 Automatic LiveUpdate Off Automa LiveUpd Gets the latest protection and program update Symantec wher computer is cor to the Internet More Info Turn Or
Findings	Automatic LiveUpdate is turned off and the Virus Definitions are older than one week. **FAIL**
Item number	AV03
Title	Verify that the Antivirus software is configured to scan all Internet downloads
Evidence	 Save As Norton AntiVirus Virus Alert Help High Risk Norton AntiVirus has detected and removed a virus from your computer. Hide Details Object Name C:\Documents and...\eicar.com[1].txt Virus Name EICAR Test String Action Taken The file was automatically deleted. OK My Network Places File name: eicar.com Save as type: Text Document Save · Cancel
Findings	Test file was detected PASS

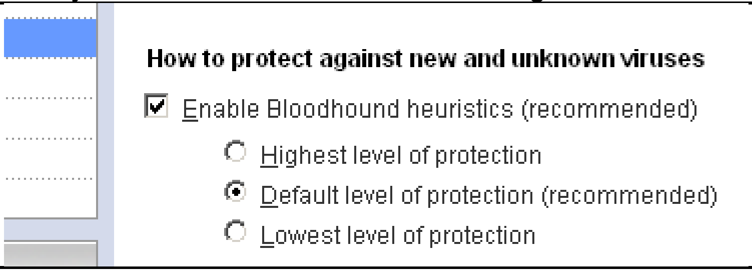
Item number	AV05
Title	Verify that the Antivirus software is configured to scan all file types.

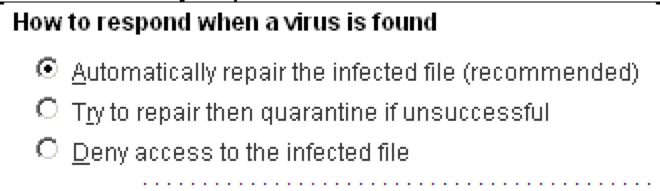
Evidence	 Which file types to scan for viruses ● Comprehensive file scanning (recommend ○ Scan files using SmartScan Customiz ☑ Scan within compressed files
Findings	All needed features are enabled PASS

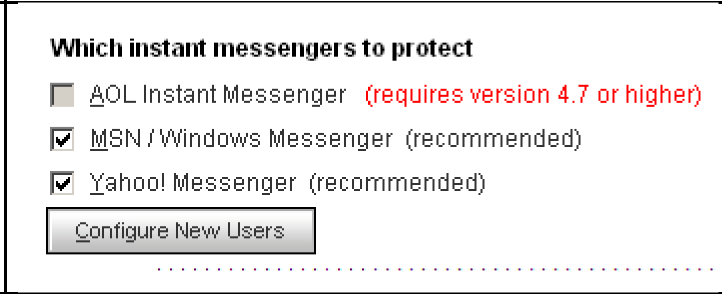
Item number	AV06
Title	Verify that Antivirus can detect malicious codes in compressed files.
Evidence	 Norton AntiVirus Virus Alert Help High Risk Norton AntiVirus has detected and removed a virus from your computer. Hide Details Object Name eicar.com Container C:\Documents an...\eicar_com[1].zip Virus Name EICAR Test String Action Taken The file was deleted. OK □ Don't alert me about this file again.
Findings	Compressed test file was detected PASS

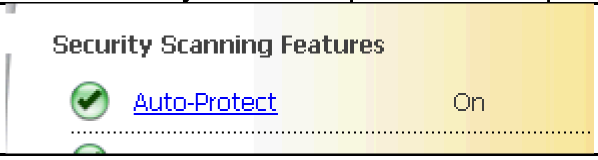
Item number	AV07
Title	Verify that the Antivirus software is configured to perform a full system scan at least once a week

Evidence	 Schedule At 8:00 PM every Fri of every week, starting 12/11/2004 Full System Scan 1/14/2005
Findings	Although a full system scan is scheduled to occur once a week, the date of the last scan is older than one week. **FAIL**

Item number	AV09
Title	Verify that the heuristic virus checking is enabled
Evidence	 **How to protect against new and unknown viruses** ☑ Enable Bloodhound heuristics (recommended) ○ Highest level of protection ● Default level of protection (recommended) ○ Lowest level of protection
Findings	Option enabled PASS

Item number	AV10
Title	Verify that the Antivirus software is configured to automatically repair infected files.
Evidence	 **How to respond when a virus is found** ● Automatically repair the infected file (recommended) ○ Try to repair then quarantine if unsuccessful ○ Deny access to the infected file
Findings	Option enabled PASS

Item number	AV11
Title	Verify that the instant messenger protection, a special feature of NAV2005, is enabled.
Evidence	 **Which instant messengers to protect** ☐ AOL Instant Messenger (requires version 4.7 or higher) ☑ MSN / Windows Messenger (recommended) ☑ Yahoo! Messenger (recommended)
Findings	All applicable options are enabled PASS

Item number	AV12
Title	Verify that the Antivirus software is configured to be automatically enabled upon PC startup
Evidence	 Security Scanning Features ✓ Auto-Protect On
Findings	Auto-Protect is (On) when examined after reboot PASS

Part 4: The Audit Report

Executive summery

The Audit was conducted with the objective of examining, and then reporting on, the state of effectiveness of the Antivirus software (Norton Antivirus 2005). The Antivirus settings, behavior, and credibility were examined and measured up to industry standards and best practices.

The Antivirus was found to be a credible commercial product that is successfully tested by industry-recognized bodies. It was also determined through our testing that the Antivirus is capable of detecting Anti-Virus test files successfully. Nonetheless, it is also our finding that the Antivirus is not configured to provide optimal protection inline with industry best practices.

The Antivirus Automatic LiveUpdate feature is turned off causing the virus definitions to be outdated. This introduces the risk of new viruses that are not-yet-recognized by the Antivirus to the system.

Although the Antivirus is configured to perform weekly full system scans, the date of the last system scan is older than one week. This indicates that the system scan is configured to occur during a time when the computer is not available (powered off). This finding introduces the risk of the Antivirus software not detecting doormat malicious code residing on the computer.

We recommend adjusting the Antivirus configuration to allow for weekly virus definition updates and weekly system scans. This will cause the Antivirus configuration, and subsequently the implementation as a whole, to be inline with industry standards and best practices.

Audit findings

The following components of the Antivirus system, Norton Antivirus 2005, were examined during this Audit:

1. The Antivirus credibility

   This was examined by researching the databases of industry-recognized bodies dedicated to Antivirus testing against in-the-wild virus lists. The testing bodies used in this Audit are ICSA Labs, the Virus Bulletin, and West Coast Labs. No failed tests for Norton Antivirus 2005 were found on any of these bodies; moreover, the Antivirus passed the ICSA Labs test in January of 2005.

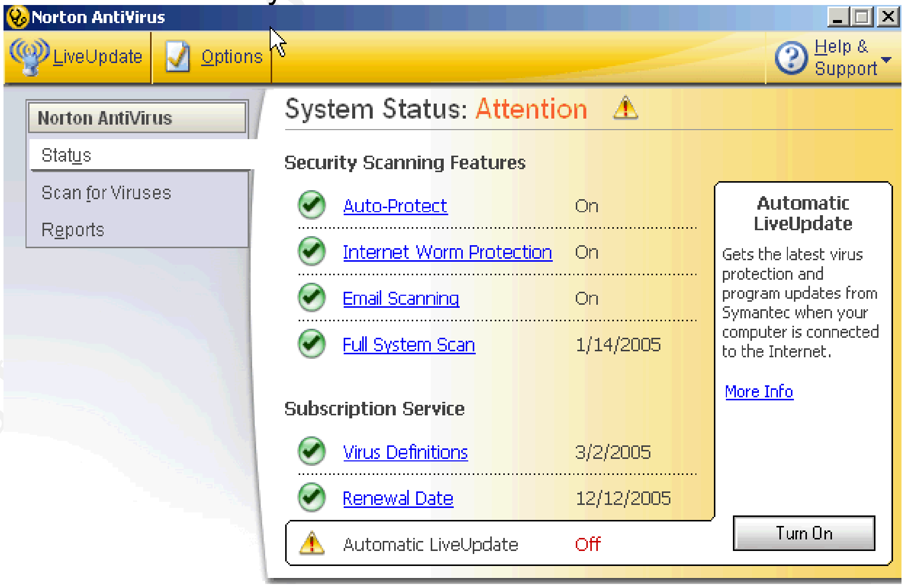
2. The Antivirus behavior

   This was examined by measuring the Antivirus behavior when tested against the Anti-Virus test files provided by EICAR (**E**uropean **I**nstitute for **C**omputer **A**ntivirus **R**esearch) and by examining the state of the Antivirus after a computer reboot. The Antivirus passed all of our behavior tests detecting all Anti-Virus test files and maintaining a secure state after a computer reboot.

3. The Antivirus configuration

   This was examined by viewing the setting screens of the Antivirus software to ensure configuration compliance with industry standards and best practices. In two separate cases, the Antivirus settings were found to be lacking as described below:

a. The Antivirus Automatic LiveUpdate feature is turned off causing the virus definitions to be outdated. This introduces the risk of new viruses that are not-yet-recognized by the Antivirus to the system.



System Status: Attention

Security Scanning Features

Auto-Protect On

Internet Worm Protection On

Email Scanning On

Full System Scan 1/14/2005

Subscription Service

Virus Definitions 3/2/2005

Renewal Date 12/12/2005

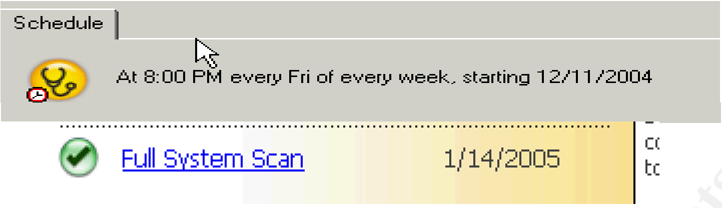
Automatic LiveUpdate Off

Automatic LiveUpdate

Gets the latest virus protection and program updates from Symantec when your computer is connected to the Internet.

More Info

b. Although the Antivirus is configured to perform weekly full system scans, the date of the last system scan is older than one week. This indicates that the system scan is configured to occur during a time when the computer is not available (powered off). This finding introduces the risk of the Antivirus software not detecting doormat malicious code residing on the computer.



Audit recommendations

Below are general recommendations to maximize the value of the Antivirus software by increasing the effectiveness of the software and reducing its vulnerability.

1. Inform Antivirus software users of industry standards and best practices.
2. Implement an automated process to ensure that the virus definitions are updated regularly; at least once a week.
3. Implement an automated process, a manual process, or both to ensure a full system scan is performed at least once a week.

All of the above mentioned recommendations require a marginal cost to implement when compared to the cost of reduced confidentiality, integrity, and availability of the data stored on the target computer.

References

CERT.org (n.d.). *Task 1 Checklist: Install and use an anti-virus program (the DURCH tests).* Retrieved March 12, 2005, from http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist1.pdf

Eicar. (2004). *The Anti-Virus test file*. Retrieved January 19, 2005, from http://www.eicar.org/anti_virus_test_file.htm

EnterpriseIT. (n.d.). *Anti-virus Checklist.* Retrieved January 19, 2005, from http://www.enterprise-itm.com/AVChecklist.htm

Gordon, S., & Howard, F. (2000). *Antivirus Software Testing for the New Millennium.* Retrieved March 12, 2005, from http://csrc.nist.gov/nissc/2000/proceedings/papers/038.pdf

ICSA Labs (2005). *ICSA Labs AV Laboratory Testing Report for January 2005.* Retrieved March 12, 2005, from http://www.icsalabs.com/html/communities/antivirus/notes/tr0105.shtml

ICSA Labs (2005). *The ICSA Labs Anti-Virus Lab Reports: Posted Monthly by ICSA Labs.* Retrieved March 12, 2005, from http://www.icsalabs.com/html/communities/antivirus/labs.shtml#2005

Krutz, R. & Vines, R. (2003). *The CISSP Prep Guide*. Indianapolis, IN: Wiley Publishing, Inc.

Miastkowski, S. (2003, January). Step-By-Step: Set Antivirus Software for Maximum

Protection [electronic version]. *PC World Magazine*.

PC Pitstop (n.d.). *Protect Your PC: Five-Step Guide*. Retrieved March 12, 2005, from http://www.pcpitstop.com/antivirus/AVirusNotes.asp

SANS.org (2004, July 1). *Auditing Networks, Perimeters, and Systems: GSNA Practical Assignment Version 3.2.* Retrieved November 12, 2004, from https://portal.sans.org/certs/GSNA0604.php

Skoudis, E., & Zeltser, L. (2003). *Malware: Fighting Malicious Code.* Prentice Hall PTR.

Virus Bulletin (2005). *Results table*. Retrieved March 12, 2005, from http://www.virusbtn.com/vb100/archives/products.xml?table

WEBtech.on.ca (n.d.).*A WEBtech Do-It-Yourself Checklist: Virus Defense Checklist.* Retrieved March 12, 2005, from http://www.webtech.on.ca/webtechantiviruschecklist.pdf

West Cost Labs (2005). *Anti-Virus Level 1***.** Retrieved March 12, 2005, from http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=1