Global Information Assurance Certification Paper

Auditing McAfee VirusScan from Auditor's Prospective
Option 1: Practical Version 3.0
GSNA Certification Attempt

Noaf Al-Bustani

May, 14th 2004

Table of Contents

Abstract

Auditing Anti-Virus software is one of the critical tasks that should take place in companies specially that are connected to the Internet. The importance of auditing Anti-Virus software is that many malicious types of software are being developed and intelligent ones are appearing more frequently these days. The days that our worries were focused on watching out for ".exe" files that are not trustworthy are gone, since then malicious software can be run without any action required from the user, as they distribute themselves, send Spam e-mails, and widen their infection without the users involvement or awareness of these activities.

In this paper, I will be discussing how to audit different features and options in McAfee VirusScan 4.5.1 SP1, since this is the Anti-Virus used in our company. The audit will include the following VirusScan features: autoupdate, autoupgrade, system scan, download scan, floppy disk scan, compressed files scan, and user action in case of infection being found. In addition, I will be auditing the controls in place to protect the features from being changed or disabled by users. The controls in VirusScan are password-protected options for all of the features mentioned before.

Introduction

Viruses are the new reoccurring pattern that has gained the most publicity recently. The media recognizes all malicious software as Viruses. Although malicious software contains many different types other than Viruses, such as Trojans horse, Worms, and other malicious software that hackers use such as rootkits.

Everyone has an Anti-Virus software, but since it is a sort of Microsoft Default, no one worries about it's functionality and rarely it has been audited.. Looking through the patterns and relationships between virus infections and abnormal internal network traffic in our company has made me realize that something is not appropriately configured in our Anti-Virus that is causing a huge number of infections among the corporate computers.

What is malicious software?

Malicious software is any software program designed to move from computer to computer and network to network to intentionally modify computer systems without the permission of the owner or operator, such as computer viruses, Trojans, and worms. These malicious software programs are created with scripting languages and enforced by Internet technologies.

The malicious software category contains three main types. The first type that everyone is familiar with is Viruses. Viruses are malicious programs that modify other host files or boot areas to replicate a few exceptions. In most cases the host is modified to include a complete copy of the malicious code program. The subsequent running of the infected host files or boot area then causes infections in other objects.

The second type of malicious software is Trojans. Trojans or Trojan horses are a non-replicating programs concealed as one type of program with its real intent hidden from the user. They do not modify or infect other files.

The third type of malicious software is Worms. Worms are a sophisticated piece of replicating code that uses it's own program coding to spread, with minimal user intervention. They typically use widely available applications such as email and chat channels to spread. Worms attach their selves to a piece of outgoing email or use a file transfer command between trusted systems. Worms are different than viruses in that they are viruses that run on autopilot. Worms do not need any action from the user to be able to run. Worms usually take advantage of vulnerabilities in software's and systems.

What is an Anti-Virus?

Anti-Virus program is a utility that searches a hard disk for viruses and removes any that are found. Most anti-virus programs include an auto-update feature

that enables the program to download signatures of new viruses so that it can check for the new viruses as soon as they are discovered.

The Anti-Virus program that I will be auditing is McAfee VirusScan 4.5.1 SP1, since this is the anti-virus that is used as the front interface for detecting, cleaning, protecting, and deleting infected files with malicious software.

McAfee's Audited Features and Options

McAfee VirusScan has many features and options. The main programs that Network Associates has included in VirusScan 4.5.1 SP1 are: **VirusScan**, **VirusScan Console**, **Create Emergency Disk**, and **VirusScan Alerting Configuration**. The features that mostly concern auditors are VirusScan Console and VirusScan. Each feature has it's own sub-programs associated with it.

The **VirusScan Console** main categories that will be audited in this practical are: VShield, AutoUpdate, AutoUpgrade, and Scan My Computer. Below are descriptions of each section:

1. *VShield* contains four tabs that are concerned with the status of different categories, which are: System Scan, E-Mail Scan, Download Scan, and Internet Filter. The two sections that will be covered in this paper are System Scan and Download Scan.

   - The System Scan section scans files that come from any source. It can check the system for viruses each time the computer is opened, run, copy, save, rename or otherwise modify files on the hard disk, on any removable media attached to the computer, or on network drives mapped to the system. In addition, it can detect viruses each time the floppy disk is accessed or shut-down. Also, it can activate heuristic scanning, which gives the scanner the capability to detect unidentified or unclassified viruses. It contains detection, action, alert, report, and exclusion tabs.
   - The Download Scan section checks files that get downloaded from the Internet to the computer through visiting websites, FTP sites, and other Internet sites. In addition this option sets options that are needed to respond to infected e-mail attachments that get received through POP-3 or SMTP e-mail client programs such as Microsoft Outlook, Netscape Mail, or others. Download Scan has tabs such as detection, action, alert, and report.

2. *AutoUpdate* allows the download and installation of new virus definition (.DAT) files for the VirusScan software according to a set schedule, which can be configured with a password to protect it.
3. *AutoUpgrade* allows the download and installation of new program files for the VirusScan software including new scan engine versions, service pack releases,

and HotFix files according to a set schedule set, which can be configured and protected by a password to increase it's security.

4. *Scan My Computer* sets the drives that need to be scanned, with enabling scanning of compressed files. Also, can enable heuristic scanning of files and programs feature to enhance the scanning capabilities of the VirusScan, which can be password protected as well as the previously mentioned features.

The **Virus Scan** feature has two modes of scanning: the classic and advanced mode. The classic mode has three sub categories: Where & What, Action, and Report. The Advanced mode includes the following sub categories: Detection, Action, Alert, Report, and Exclusion. Each mode will be explained in detail below.

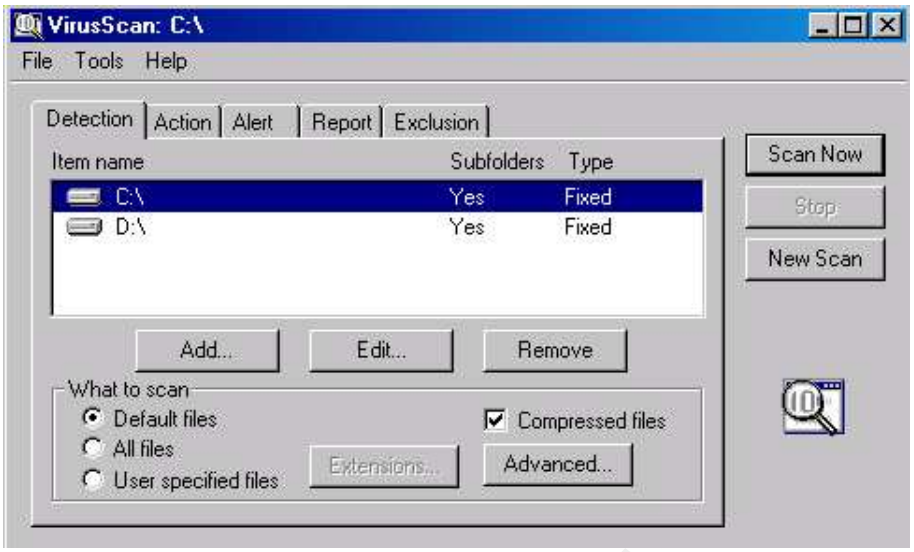
The Classic mode (Figure 1) includes the simple scanning features such:

Figure 1: Classic Mode

- Where & What: gives the user the option to scan the folder/hard drive and can include the subfolders and compressed files. It allows you to scan specified default files, all files, or user specified files.
- Action: allows the user to choose the action taken after an infection is found. The options listed are prompt user for action, clean, move, delete, and continue scanning.
- Report: is the field that locates the folder where the log file will be saved and asks to limit the size of the log file. In addition, this option customizes the display message to be viewed when an infection is detected and has an additional option to sound an alert upon infection or not.

The Advanced mode (Figure 2) includes the following features:

Figure 2: Advanced Mode



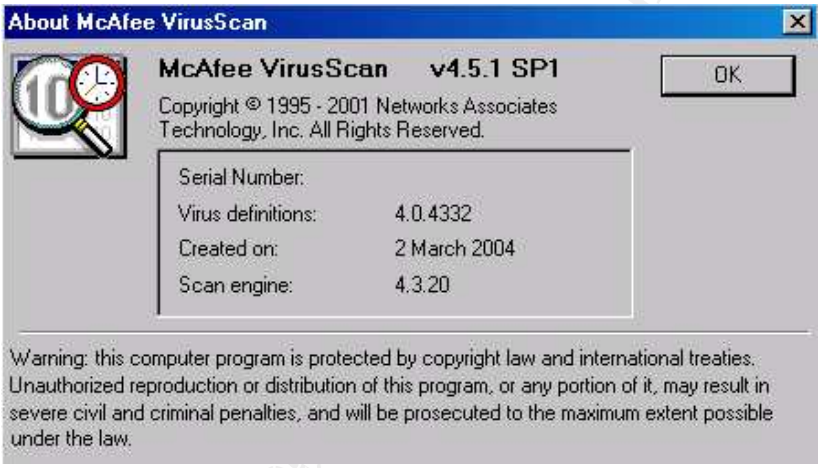
- Detection: includes the same option as the "Where & What" in the classic mode with the addition of an advanced section for scanning choice. The Advanced scan settings section includes the heuristic scanning option. The heuristics scan settings if enabled provides three choices: enable macro heuristics scanning, enable program file heuristics scanning, enable macro and program file heuristics scanning.
- Action: is similar to the classic mode action field with the addition of the ability to select or deselect the actions such as clean, delete, continue, stop, exclude, and move infected file.
- Alert: includes the customization of display message, sound alert option, and notify alert manager option.
- Report: includes the logging file options such as location of log file, what to log (virus detection, virus cleaning, infected file deletion, session settings, session summary, date and time) and has the option to limit the log file size.
- Exclusion: gives the administrator the choice to exclude any folders from being scanned.

Part 1: Research in Audit, Measurement Practice, and Control

Audit Scope

The practical is focused on Auditing Mcafee VirusScan Version 4.5.1 SP1 (Figure 3) running on Windows 2000 Professional Operating System with SP4 installed and all the latest updates available from Microsoft. The main function of Mcafee Anti-Virus is to protect the company's desktops from Worms, Viruses, and Trojans.

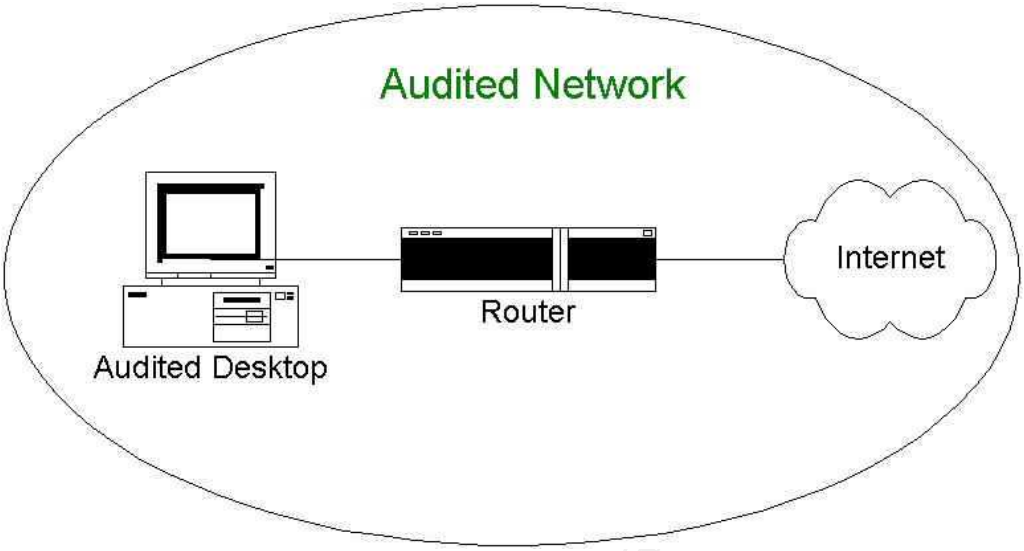
Figure 3: McAfee VirusScan Version



The purpose of Auditing Mcafee Anti-Virus software is due to the fact that recently the company's computers have been getting infected with many Worms and Viruses. Also, the company's internal e-mail has been getting many Spam e-mails that include infected attachments sourced from internal IP addresses. In addition, it has been detected a lot of internal attacks on our network due to the infection of some PCs.

The importance of the audit is that the company's computers are all connected to the Internet, which makes malicious software a huge danger to the corporate computers and network. In addition, the core function of the company is based on exchanging emails with customers and other internal departments and that makes any infection with any type of malicious software have a big effect on the reputation and trust of the company's security and image in the market and interlay within the corporate. The significance of the VirusScan is that the company's network is directly connected to the Internet to a router without any existence of firewall. Figure 4 displays a diagram with the structure of the network.

Figure 4: Network Diagram



Risk Evaluation

The most significant risk is being infected with malicious software that sends Spam emails to other employees or customers. Also, some malicious software have been causing internal attacks on the network and generating abnormal traffic that has made the company's IDS detect illegal activities from employees unintentionally. The infection of files negatively affects the confidentiality of the data residing on the infected computers. In addition, it harmfully affects the availability of the service of the server or application that got infected by malicious software. The overall evaluation of the risks is high as is illustrated in the threat table.

The Threat Table

Threat No.	Threat	Capacity to inflict damage
1	Damage or modification of sensitive information/data caused by infection by malicious software. (Threat to availability and Integrity)	70%
2	Loss of Customer trust and reputation in the market by sending infected e-mails and confidential files to customers or other users. (Threat to Confidentiality)	60%
3	Unavailability of system due to infection specifically if the computer contains core applications. (Threat to availability)	40%
4	Internal network attacks and heavy load on company's IDS caused by infected systems and increase network	60%

	traffic and cause heavy load on the internal firewall that could cause denial of service. (Threat to availability)	
5	Disabling the scanning of Anti Virus caused by unaware employees.	80%

The main information assets that will be affected by a malicious software infection, is data files such as core applications, e-commerce services, confidential documents and data that are proprietary of the company as is illustrated in the assets table. The data files can be corrupted and lose their integrity. In addition, data files can contain confidential information, which the infection might lead to the disclosure of this information.

Assets Table

Asset No.	Asset Sub categories
1	Core Applications
2	E-commerce services
3	Confidential data/file of the company

The vulnerabilities have high degree of exposure and high potential impact. The vulnerability table shows the vulnerabilities, degree of exposure, and potential impact.

Vulnerability Table

Vulnerability No.	Vulnerability	Degree of Exposure	Potential Impact
1	Out dated VirusScan definition and DAT files.	High	High
2	VirusScan not configured securely (not password protected)	High	High
3	VirusScan not configured properly (disabled scanning of files, attachments, e-mails, or download)	High	High
4	Desktop computers not scanned for malicious software.	High	High
5	Un-patched operating system or email server and exchanged with the latest updates and fixes.	High	High

Current State

The search included web sites, search engines, anti-virus vendors, and SANS reading room. The major results included generic checklists and best practices to

secure computers from viruses. The search terms that were used during this phase are: anti-virus checklist, anti-virus security, anti-virus configuration, Mcafee security, Mcafee VirusScan security, and VirusScan checklist. The search results gave valuable starting point in creating an audit checklist.

The anti-virus vendors that the search included were: Mcafee, Trend Micro, and Symantec. These vendors had specific best practices to anti-virus checklist that some of the items listed were applicable to McAfee VirusScan and other checklist items were specific to the vendor's software. These items were considered a guide in developing the audit checklist.

There were few books that had some best practices related to anti-viruses and mostly prevention and protection from malicious software. The best practices were related to floppy disks, Internet explorer options (configuring Internet zones), and downloading freeware. These practices are useful in helping to come up to checklist items in addition to the previously found.

The references section is divided into two sections according to the type of information found in the reference. The web site based references include checklists of securing computers from viruses, while the book based references include best practices.

Web Sites References

WEBtechan Internet Presence Provider, "Virus Defense Checklist" available at http://www.webtech.on.ca/WebtechAntiVirusChecklist.pdf

Network Associates network security and availability technology, "Anti-Virus Health Check Assessment – Security Consulting Service by Network Associates Inc. " available at http://www.networkassociates.com/us/services/security/assessment/av_health_check.htm

SurferBeware.com, "Antivirus Checklist" available at http://viruses.surferbeware.com/antivirus-checklist.htm

Enterprise IT IT management solution,"Anti-Virus checklist" available at http://www.enterprise-itm.com/AVChecklist.htm

CERT/Coordination Center reporting center for Internet Security problems," Task 1 Checklist - Install and use an anti-virus program" available at http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist1.pdf

Books References

Shea, Brian. Have You Locked the Castle Gate? Home and Small-Business Computer Security. O'Reilly, August 2001.

Grimes, Roger. Malicious Mobile Code: Virus Protection for Windows. O'Reilly, August 2001.

Part 2: Create an Audit Checklist

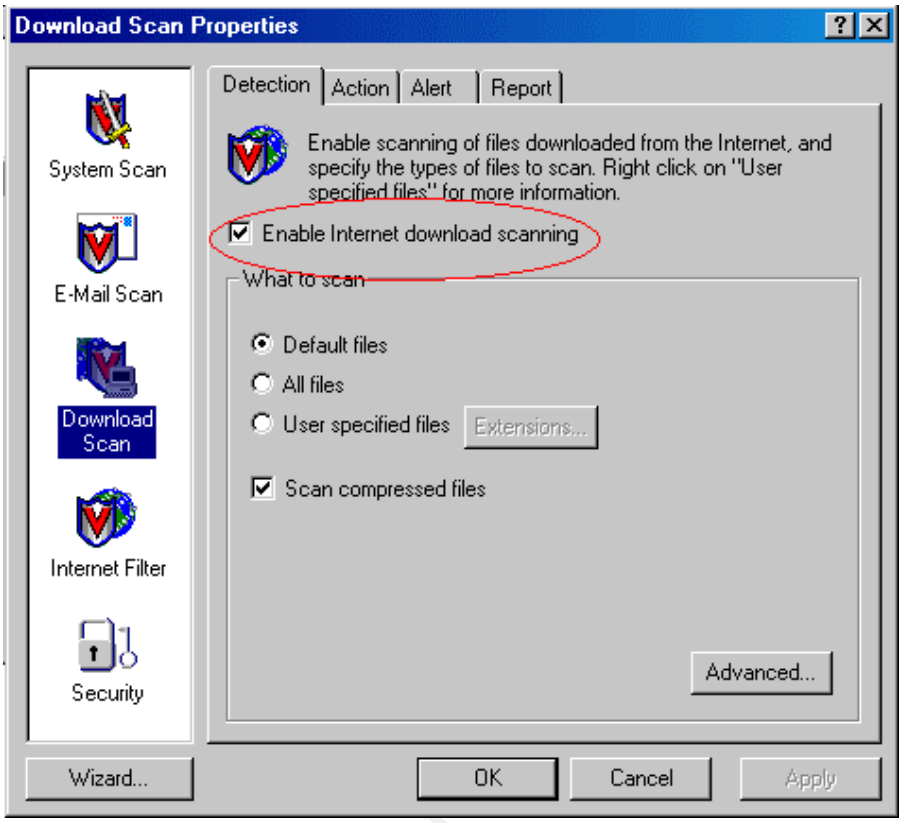
Audit Checklist

Item Number 1: Verify that Download Scan is enabled.

- Risk: downloading infected software or any type of files that can get distributed throughout the company's network (High)
- Compliance: Pass or Fail
- The Compliance Criteria is that the test would pass if the VirusScan does not allow the downloading of infected files to the computer. Fail would be assigned if the VirusScan does not detect that an infected file is being downloaded onto the computer.
- Test Nature: Objective
- Control Objective: determine that the VirusScan is scanning all downloaded file before saving them to the computer and prompting the user of action in case of downloading infected file.
- Reference: Surferbeware.com, "AntiVirus Checklist", http://viruses.surferbeware.com/antivirus-checklist.htm
- Testing Procedure:

    1. Go to start
    2. Click on programs
    3. From the list of programs select "Network Associates"
    4. The "Network Associates" program has four sub programs.
    5. Select the "VirusScan Console"
    6. Right click on the "VShield"
    7. Select "properties" then click on "Download Scan".
    8. Verify that the "disabled" button is shaded that means that the option is "enabled". See Figure 5

Figure 5: Download Scan Properties



Item Number 2: Verify that System Scan is enabled.

- Risk: VirusScan not detecting an infected files or folder (High), because if the system scan is not enabled that indicates that the computer is not constantly scanning files residing on the system, which means that any malicious software could be residing on the computer without being detected.
- Test Nature: Objective
- Control Objective: determine that the VirusScan is scanning system files while the computer is turned on.
- Compliance: Fail or Pass
- Compliance Criteria: The test would be marked as pass if the system scan option is enabled and does scan files on the computer. Fail will be marked if system scan does not detect infected files on the computer.
- Reference: "Top 10 Tips to Keep Your Computer Virus-Free", http://viruses.surferbeware.com/antivirus-tips.htm
- Testing Procedure:

1. Go to start
2. Click on programs
3. From the list of programs select "Network Associates"
4. The "Network Associates" program has four sub programs.
5. Select the "VirusScan Console"
6. Right click on the "VShield"

7. Click on “System Scan Status”
8. Then click on “Properties”
9. Verify that the “Enable system scan” is marked. See Figure 6

Figure 6: System Scan Properties

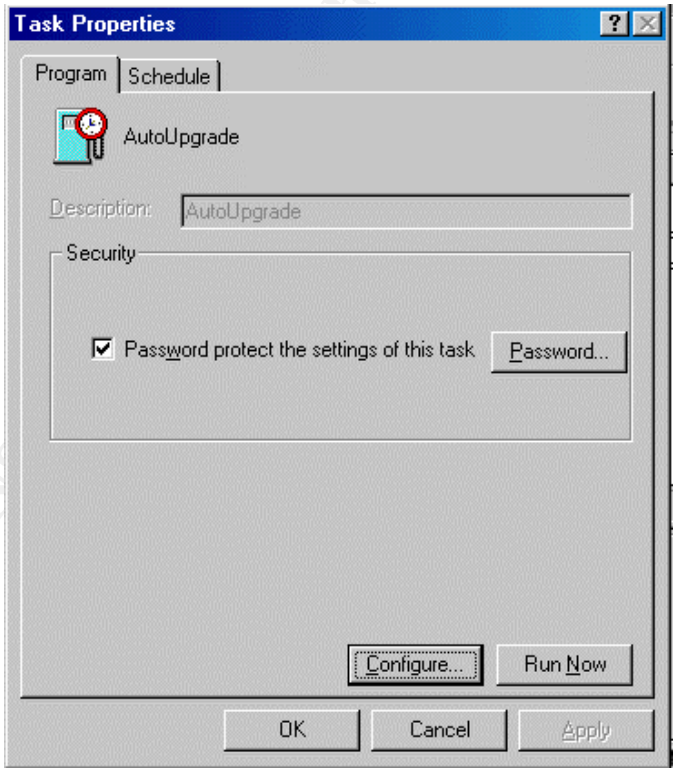
Item Number 3: Verify that Schedule and Configure of “AutoUpgrade” is password protected

- Risk: VirusScan not having the latest upgrades Anti-Virus software that Network Associates issued (Medium), the danger of being able to change the schedule or configuration of the "autoupgrade" is that the user can disable upgrading the VirusScan which means not being able to download and install new program files, including new scan engine versions, service packs, and hot fixes files.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be assigned if the "AutoUpgrade" does not allow any user with the appropriate password to change the configuration of the option. Fail will be marked if any user without the appropriate password can change the configuration of the "AutoUpgrade" option.
- Test Nature: Objective

- Control Objective: determine that the autoupgrade is properly configured to upgrade on a daily basis and that the configuration options are not accessed without a valid password.
- Reference: Inspired by Network Associates Inc., "Anti-Virus Health Check Assessment" found at http://www.networkassociates.com/us/services/security/assessment/av_health_check.htm
- Testing Procedure:

1. Go to start
2. Click on programs
3. From the list of programs select "Network Associates"
4. The "Network Associates" program has four sub programs.
5. Select the "VirusScan Console"
6. Right click on the "AutoUpgrade"
7. Select "Properties"
8. Verify that the "password protect the settings of this task" button is clicked. See Figure 7

Figure 7: Task Properties (AutoUpgrade)

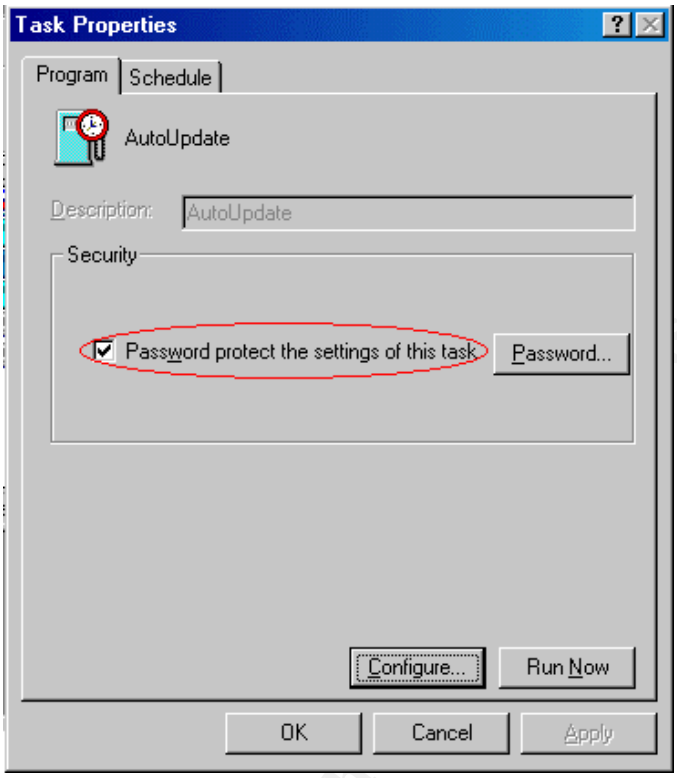


Item Number 4: Verify that Schedule and Configure of “AutoUpdate” is password protected

- Risk: out of dates virus signatures (High), due to the fact that disabling Autoupdate or changing it's configuration will cause great danger to the computer since Autoupdate downloads and installs the new virus definitions (.DAT) files to the VirusScan software which protects the computer from new viruses and other malicious software.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be assigned if the "AutoUpdate" does not allow any user with the appropriate password to change the configuration of the option. Fail will be marked if any user without the appropriate password can change the configuration of the "AutoUpdate" option.
- Test Nature: Objective
- Control Objective: determine that the autoupgrade is properly configured to upgrade on a daily basis and that the configuration options are not accessed without a valid password.
- Reference: Inspired by Network Associates Inc., "Anti-Virus Health Check Assessment" found at http://www.networkassociates.com/us/services/security/assessment/av_health_check.htm
- Testing Procedure:

    1. Go to start
    2. Click on programs
    3. From the list of programs select “Network Associates”
    4. The “Network Associates” program has four sub programs.
    5. Select the “VirusScan Console”
    6. Right click on the “AutoUpdate”
    7. Select “Properties”
    8. Verify that the “password protect the settings of this task” button is selected. See Figure 8

Figure 8: Task Properties (AutoUpdate)



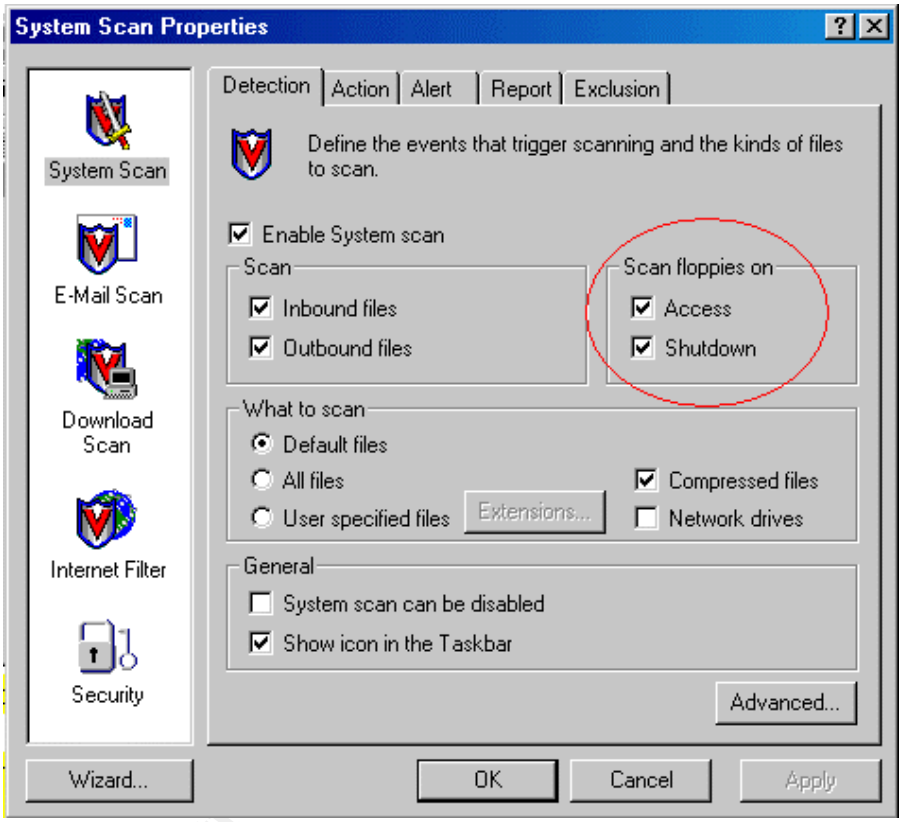
Item Number 5: Verify that VirusScan Scans Floppy Disks

- Risk: VirusScan unable to detect infected files residing on Floppy Disks (High), because all the corporate computers have Floppy Disks and they might be carrying infected files that can be transferred to the network and other computers in the company if the VirusScan does not scan Floppy Disks when inserted or a shutdown is taking place.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be assigned as a result if the VirusScan detects infected file while inserting the Floppy Disk or when shutdown has taken place. Fail will be assigned if the VirusScan does not detect any infection while inserting the Floppy Disk or through shutting down the computer.
- Test Nature: Objective
- Control Objective: verify that VirusScan scans Floppy Disks upon insertion and shutdown of the computer and accessing the floppy disk.
- Reference:" Top 10 Tips to Keep Your Computer Virus-Free", http://viruses.surferbeware.com/antivirus-tips.htm
- Testing Procedure:

    1. Go to start
    2. Click on programs
    3. From the list of programs select "Network Associates"
    4. The "Network Associates" program has four sub programs.
    5. Select the "VirusScan Console"

6. Right click on the “VShield”
7. Click on “System Scan Status”
8. Click on “Properties”
9. Verify that “Scan floppies on access and shutdown” options are marked. See Figure 9

Figure 9: System Scan Properties (Scan Floppies)



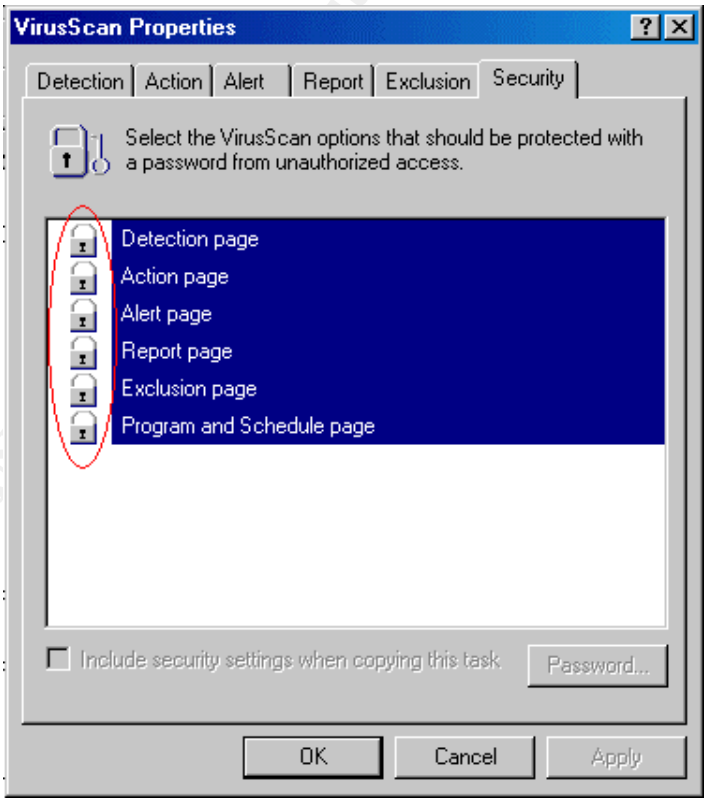
Item Number 6: Verify that "Scan my Computer" is password protected

- Risk: users disabling scanning of compressed files or heuristic scanning or changing any of the "Scan my Computer" configuration (High), because if the user changes the configuration of "scan my computer" then can disable scanning of compressed files, and disable heuristic scanning of programs and files, which will cause the VirusScan not to be able to detect infected compressed files or macros.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be marked if the user enters an invalid password will not be able to change any option in the "Scan my Computer" section. Fail will be assigned if the user enters an invalid password and is able to change the options in the "Scan my Computer" section.
- Test Nature: Objective

- Control Objective: determine that the "Scan my computer" is properly configured to scan the computer's hard drive daily and that the configuration options are not accessed without a valid password.
- Reference: TechRepublic part of CNET Networks a global media company, “Virus Prevention Checklist” available at http://techrepublic.com.com/5138-6321-730102.html?tag=search
- Testing Procedure:

1. Go to start
2. Click on programs
3. From the list of programs select “Network Associates”
4. The “Network Associates” program has four sub programs.
5. Select the “VirusScan Console”
6. Right click on the “Scan My Computer”
7. Click on “Properties”
8. Click on the "configure" icon.
9. Then select the "Security" section
10. Verify that the lock icon is closed on all of the options listed in the security section. See Figure 10

Figure 10: VirusScan Properties

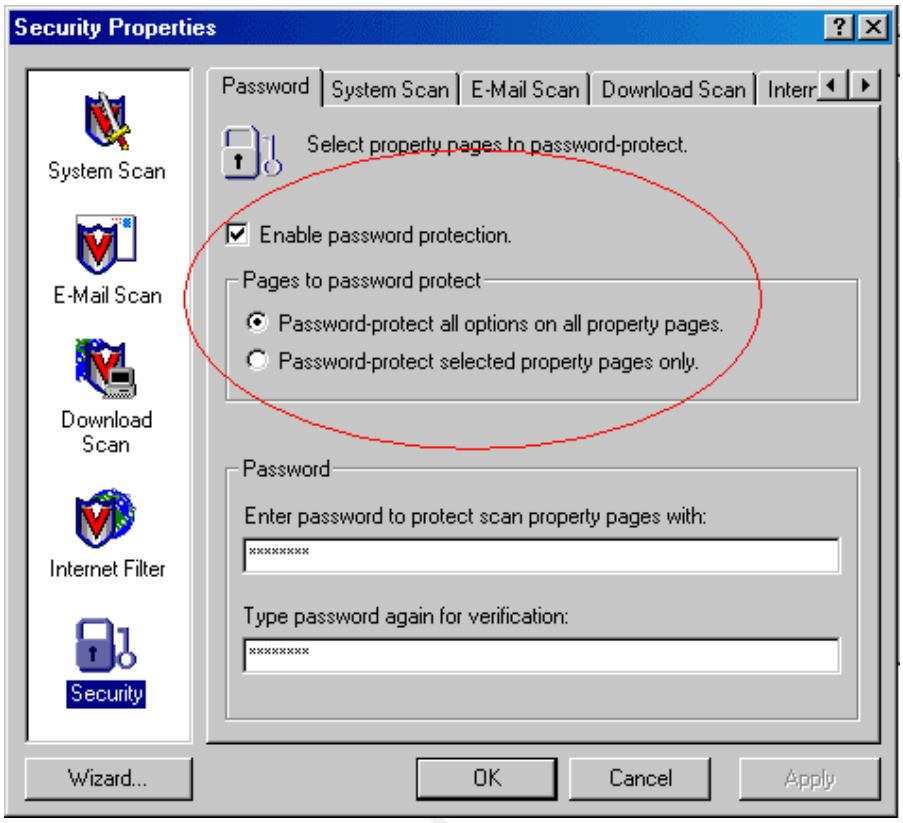


Item Number 7: Verify that Download Scan is password protected

- Risk: users disabling the feature of scanning downloaded files (High), due to that disabling download scan will cause the VirusScan not able to scan files while downloading them from the Internet that could be infected.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be marked if the user with wrong password will be not be able to change any option in the "Download Scan" section. Fail will be assigned if the user enters invalid password and be able to change the options in the "Download Scan" section.
- Test Nature: Objective
- Control Objective: determine that the download scan is properly configured to download all files including compressed files and that the configuration options are not accessed without a valid password.
- Reference: Surferbeware.com, "AntiVirus Checklist", http://viruses.surferbeware.com/antivirus-checklist.htm
- Testing Procedure:

1. Go to start
2. Click on programs
3. From the list of programs select "Network Associates"
4. The "Network Associates" program has four sub programs.
5. Select the "VirusScan Console"
6. Right click on the "VShield"
7. Click on "Properties"
8. Click on the "Properties" icon in the "Download Scan" section
9. Select the "Security" tab in the left panel.
10. Verify that the "enabled password protection" is marked. See Figure 11

Figure 11: Security Properties



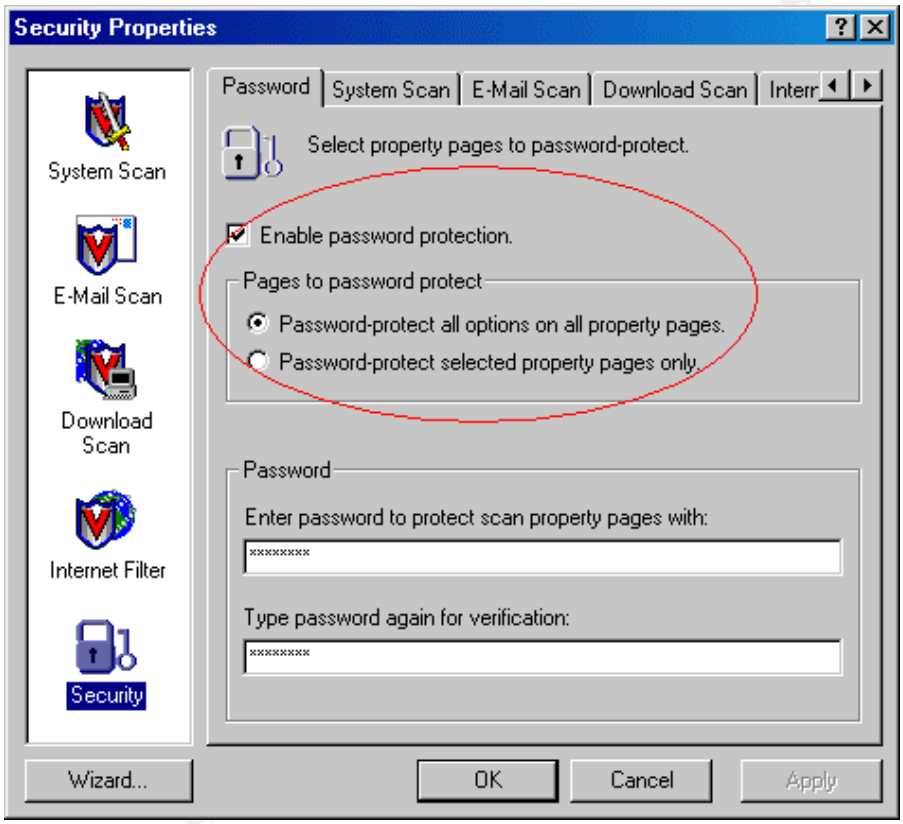
Item Number 8: Verify that System Scan is password protected

- Risk: users mis-configuring system scan by disabling it the option (Medium), which will cause any infection not to be found if the user changes the configuration of the System Scan without a valid password.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be marked if a user with an invalid password will not be able to change any option in the "System Scan" section. Fail will be assigned if a user with an invalid password is able to change the options in the "System Scan" section.
- Test Nature: Objective
- Control Objective: determine that the system scan is properly configured to scan all type of files and that the configuration options are not accessed without a valid password.
- Reference: TechRepublic part of CNET Networks a global media company, "Virus Prevention Checklist" available at http://techrepublic.com.com/5138-6321-730102.html?tag=search
- Testing Procedure:

    1. Go to start
    2. Click on programs
    3. From the list of programs select "Network Associates"
    4. The "Network Associates" program has four sub programs.

5. Select the “VirusScan Console”
6. Right click on the “VShield”
7. Click on “Properties”
8. Click on the "Properties" icon in the "System Scan" section
9. Select the "Security" tab in the left panel.
10. Verify that the "enabled password protection" is marked. See Figure 12

Figure 12: Security Properties (Password Protection)

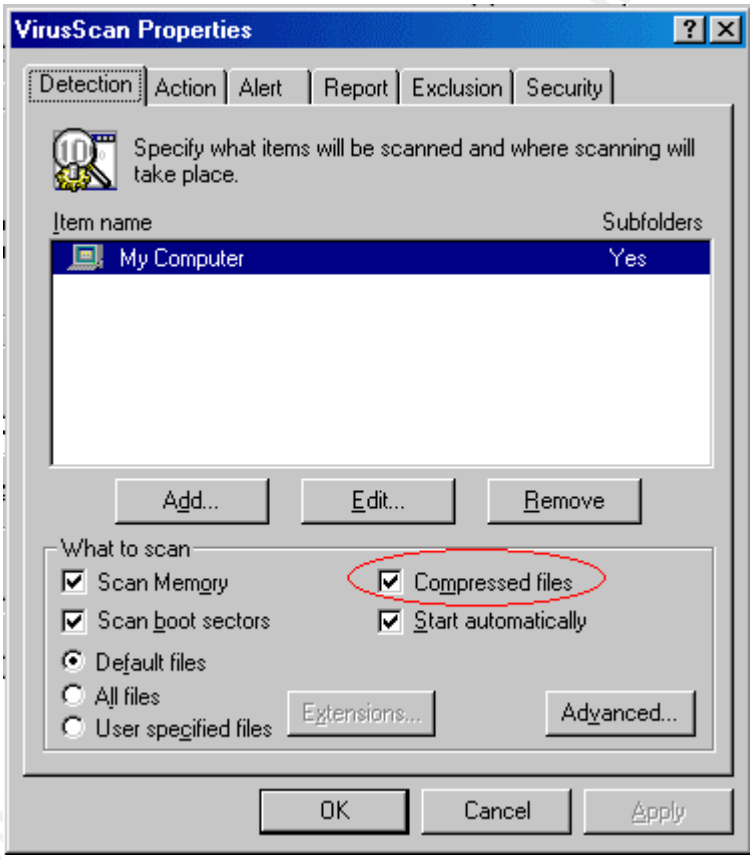


Item Number 9: Verify that VirusScan scans compressed files

- Risk: users disabling the scanning of compressed files (High), due to that compressed files can contain infections.
- Compliance: Pass or Fail
- Compliance Criteria: Pass will be granted if the VirusScan detects an infected compressed file (zipped file or folder). Fail will be granted if the VirusScan does not detect infected file or folder that is infected.
- Test Nature: Objective
- Control Objective: verify that VirusScan properly scans compressed files and the configuration options are not accessed without a valid password.
- Reference: Info Packaging company, "Virus Prevention Checklist" at http://www.infopackaging.com/Brochures/virusprevention.doc
- Testing Procedure:

1. Go to start
2. Click on programs
3. From the list of programs select "Network Associates"
4. The "Network Associates" program has four sub programs.
5. Select the "VirusScan Console"
6. Right click on the "Scan My Computer"
7. Click on "Properties"
8. Click on "Configure"
9. Check that "Compressed files" is marked in the VirusScan Properties (Detection Section). See Figure 13

Figure 13: VirusScan Properties (Detection)



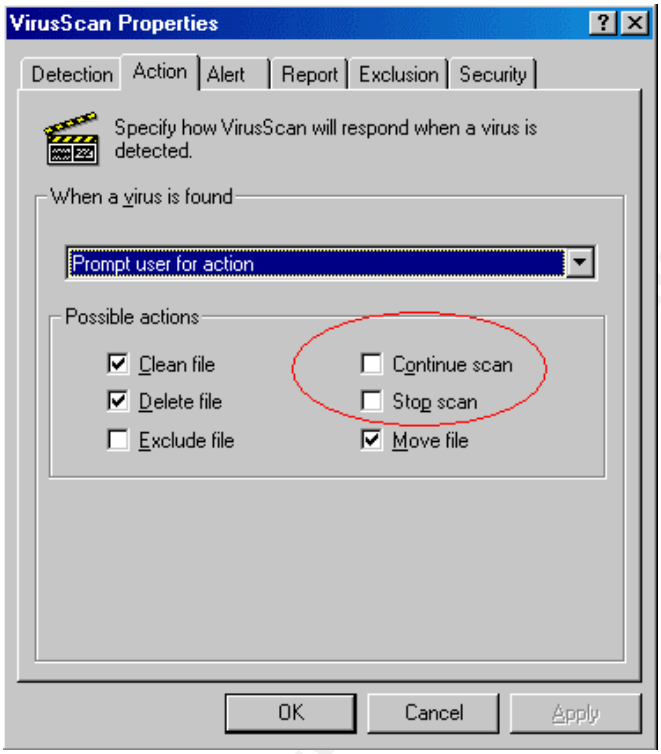
Item Number 10: Verify that the user does not have the option to "Continue scan" or "Stop Scan"

- Risk: user can select continue or stop scanning as an action and infection remains on the computer (High), because continuing or stopping the scan does not clean, delete the infected files which means that the malicious software will be residing in the system.
- Compliance: Pass or Fail

- Compliance Criteria: Pass will be assigned if the VirusScan detects an infection and does not prompt the user to continue scan or stop scan file options. Fail will be assigned if the user will be able to select continue or stop scan options.
- Test Nature: Objective
- Control Objective: verify that the user does not have the option to stop or continue the scan after an infection is found.
- Reference: TechRepublic part of CNET Networks a global media company, “Virus Prevention Checklist” available at http://techrepublic.com.com/5138-6321-730102.html?tag=search
- Testing Procedure:

    1. Go to start
    2. Click on programs
    3. From the list of programs select “Network Associates”
    4. The “Network Associates” program has four sub programs.
    5. Select the “VirusScan”
    6. Click on "tools", then make sure to select "Advanced" to change the VirusScan mode to the “Advanced Mode” from the “Classic Mode”.
    7. Click on the "Action" sections
    8. Verify that options "Continue Scan" and "Stop Scan" should be cleared. See Figure 14

Figure 14: VirusScan Properties (Action)



Part 3 - Conduct the Audit - Testing, Evidence and Findings

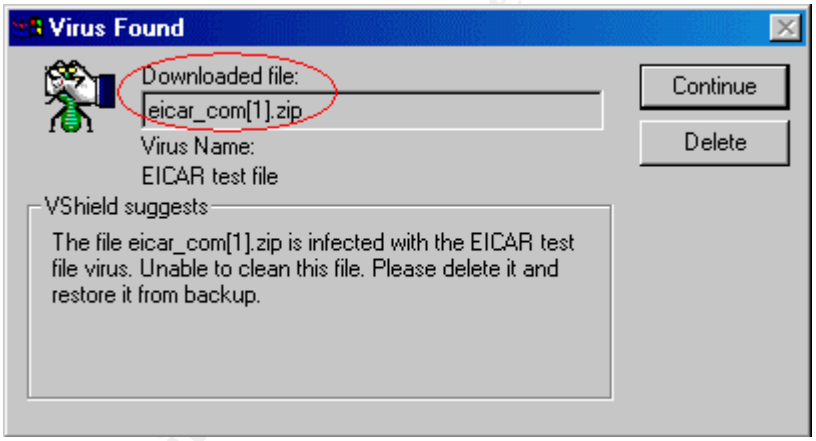
Item Number 1: Verify that Download Scan is enabled ☑

Compliance: Pass

Stimulus/Response:

1. Download the file Eicar.com.zip from http://www.eicar.org/anti_virus_test_file.htm
2. You will be prompted to select an action "delete" or "continue". See Figure 15.
3. After clicking "continue", it will view to save the file or open it.
4. Click on save file.
5. The file will fail to be saved since it is detected as an infected file.

Figure 15: Virus Found (Download)



Item Number 2: Verify that System Scan is enabled. ☒

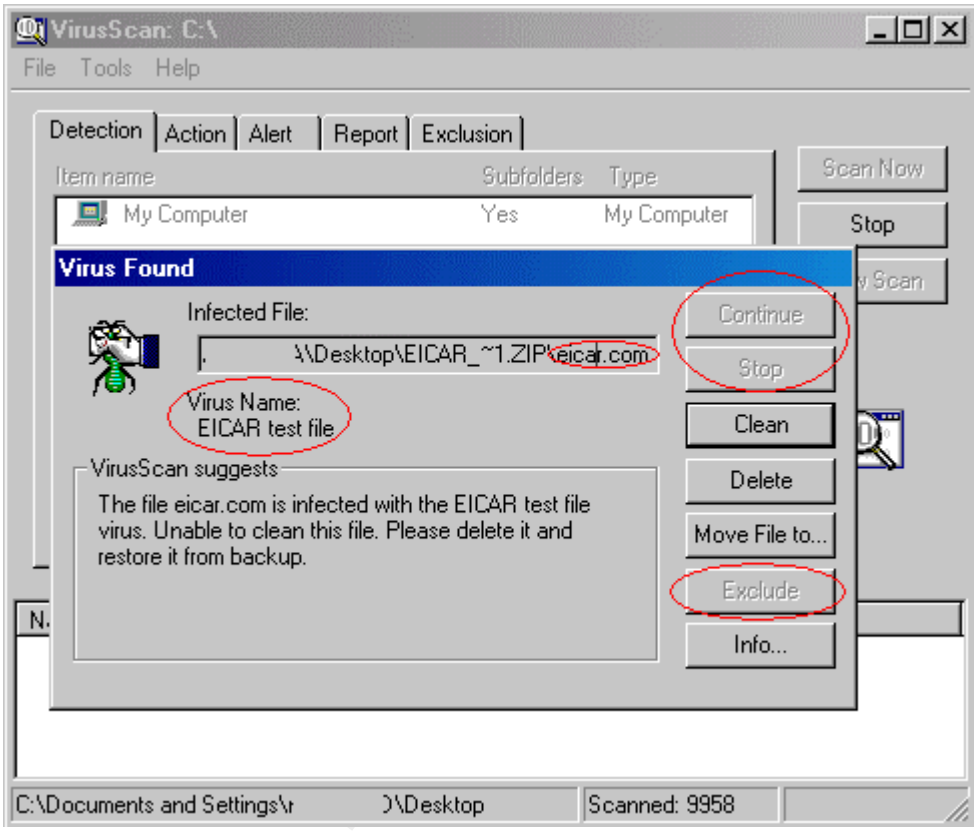
Compliance: Fail

Stimulus/Response:

1. Download the file EICAR_com.ZIP from http://www.eicar.org/anti-virus-test-file.htm
2. Save the file to the computer.
3. VirusScan does not detect that there is an infected file unless the user scans the infected file manually. Note: The file gets saved on the computer desktop and does not get detected by the VirusScan although it is enabled to scan

system files. See Figure 16 that indicated infection after manually scanning of the file.

Figure 16: Virus Found (System Scan)



Item Number 3: Verify that Schedule and Configure of "AutoUpgrade" is password protected ☑

Compliance: Pass

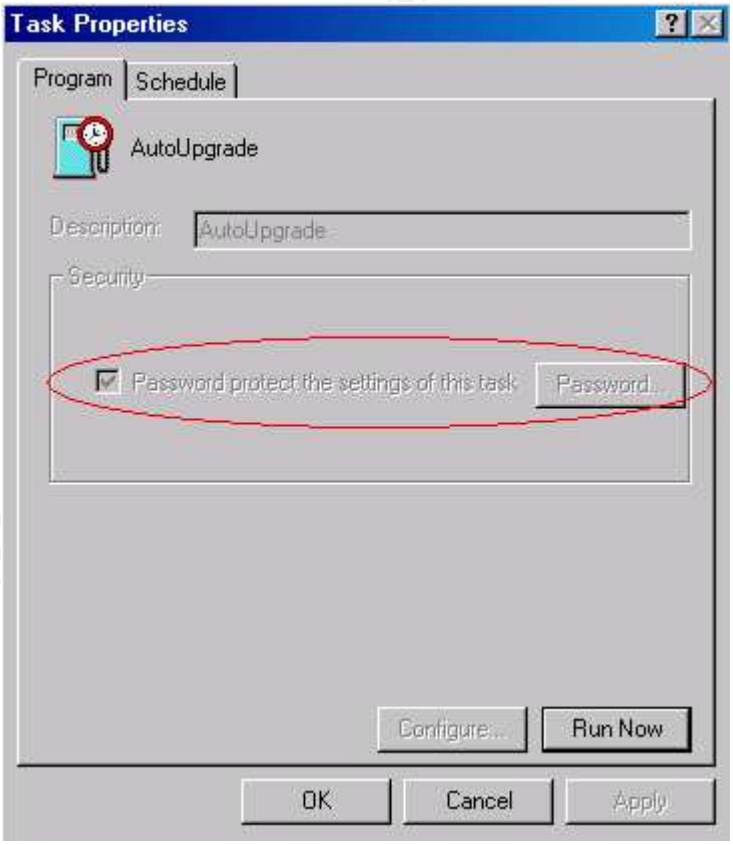
Stimulus/Response:

1. Go to start
2. Click on programs
3. From the list of programs select "Network Associates"
4. The "Network Associates" program has four sub programs.
5. Select the "VirusScan Console"
6. Right click on the "AutoUpgrade"
7. Select "Properties"
8. When get prompted for password, keep blank or enter any random password. VirusScan will display an error message prompting you that the entered password is invalid. See Figure 17.

9. Try to click on the "cancel" button. After clicking, the configuration page will be displayed but all options will be grayed out, meaning can't do any changes to the configuration or the schedule of the AutoUpgrade feature. See Figure 18.

Figure 17: AutoUpgrade (Wrong Password)

Figure 18: AutoUpgrade (Grayed Out)



Item Number 4: Verify that Schedule and Configure of “AutoUpdate” is password protected ☑

Compliance: Pass

Stimulus/Response:

1. Go to start
2. Click on programs
3. From the list of programs select “Network Associates”
4. The “Network Associates” program has four sub programs.
5. Select the “VirusScan Console”
6. Right click on the “AutoUpdate”
7. Select “Properties”
8. When prompted for a password, leave it blank or enter any random password. VirusScan will display an error message prompting you that the entered password is invalid. See Figure 19. Notice that the properties page is viewed with the option “Enable password protection” marked and all other options are grayed out. See Figure 20.
9. Try to click on the "cancel" button. After clicking, the configuration page will be displayed but all options will be grayed out, meaning can't do any changes to the configuration or the schedule of the AutoUpdate feature.
10. Click on the "Schedule" section to attempt to change the schedule, you will be prompted to enter a password. Click on the cancel button again, and then you will be able to view the schedule without being able to change any options. See Figure 21

Figure 19: AutoUpdate (Password Error)

Figure 20: AutoUpdate (Enable Password)

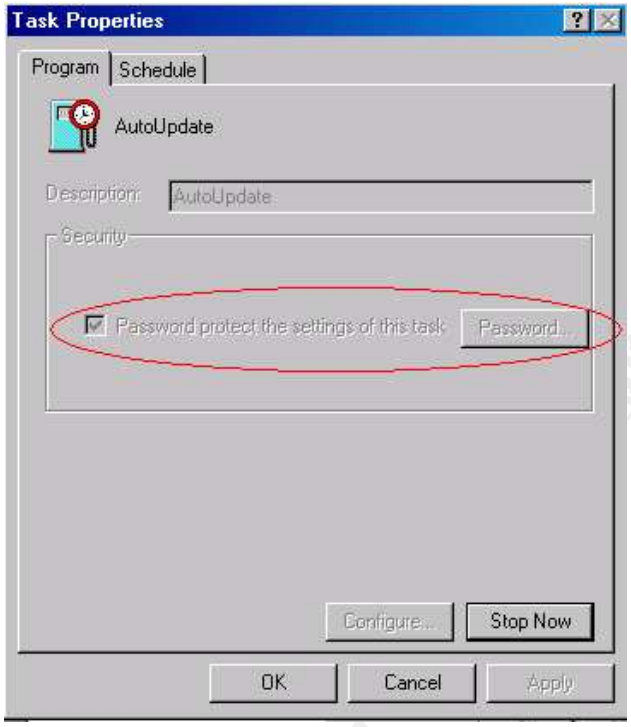
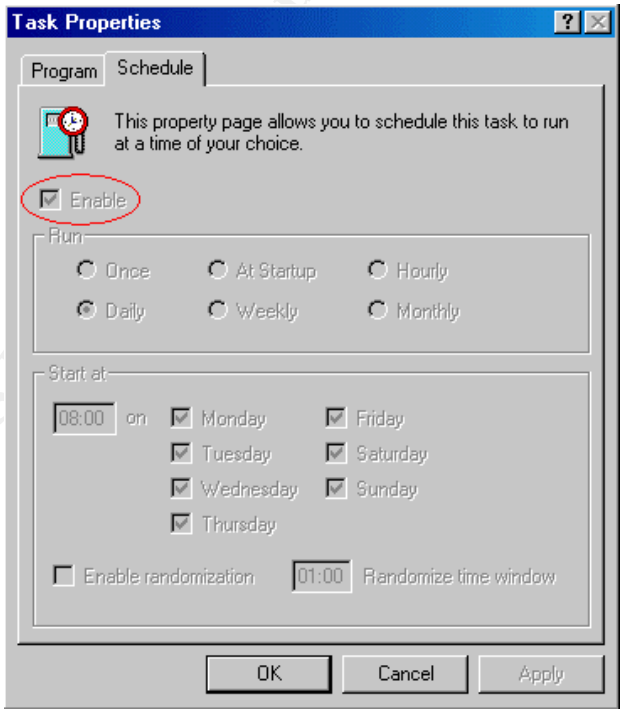


Figure 21: AutoUpdate (Schedule Password)



Item Number 5: Verify that VirusScan Scans Floppy Disks ☒

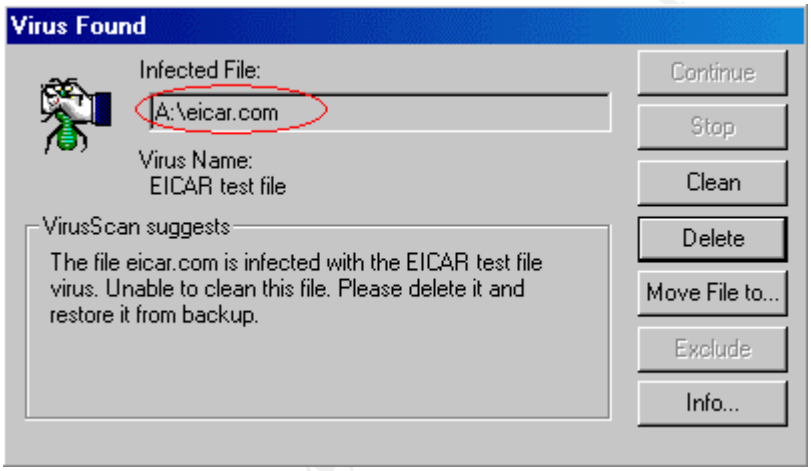
Compliance: Fail

Stimulus/Response:

1. Download Eicar.com from http://www.eicar.org/anti_virus_test_file.htm
2. In the action prompt exclude the file, to be able to save it to a Floppy Disk.
3. Remove the floppy disk and re-insert it again to verify that the VirusScan scans floppy disks on accessing.

Notice: the VirusScan does not automatically detect the infected file unless you manually choose to scan the specific file or scan the floppy disk. See Figure 22

Figure 22 Virus Found (Floppy Disk)



Item Number 6: Verify that "Scan my Computer" is password protected ☑

Compliance: Pass

Stimulus/Response:

1. Go to Start
2. Select Programs
3. Choose Network Associates
4. Select VirusScan Console
5. Right Click on "Scan My Computer" icon
6. Click on "Properties"
7. You will be prompted to enter a valid password.
8. Enter any random password and VirusScan will return an error message (See Figure 23), then click on "Ok" and see number 10.
9. Don't enter any password and click on "Cancel". See Figure 24
10. The VirusScan will let you view the properties of "System Scan" without being able to do any changes. (See Figure 25)

Notice: the “Scan My Computer” properties will view all the options grayed out, which means that you will not be able to do any changes. Just viewing mode.

Figure 23: VirusScan (Incorrect Password)

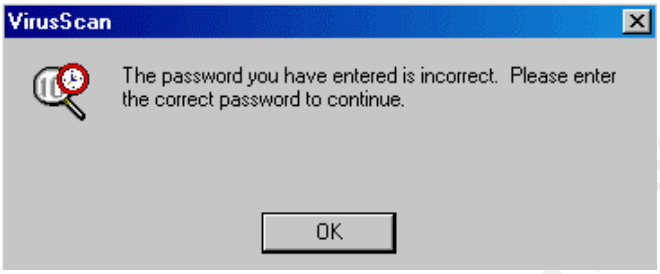
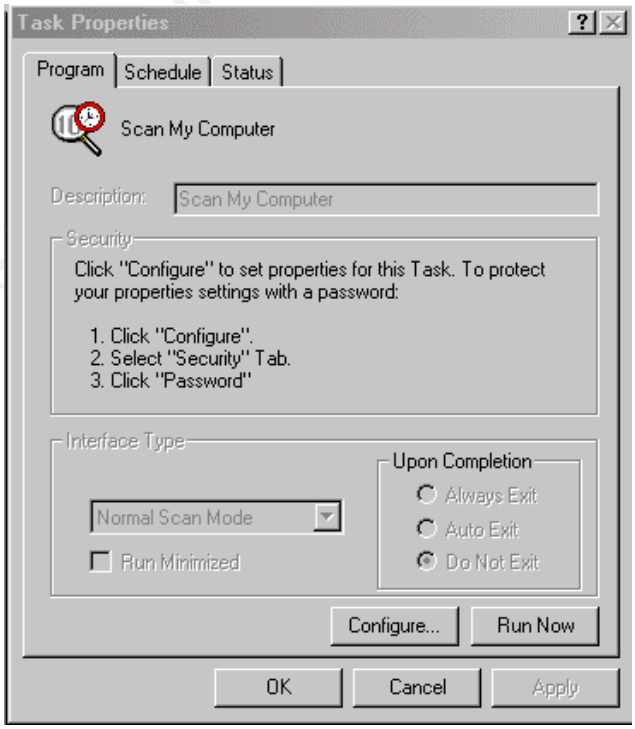


Figure 24: VirusScan (Empty Password)

Figure 25: Task Properties (Options Grayed)



Item Number 7: Verify that Download Scan is password protected ☑

Compliance: Pass

Stimulus/Response:

1. Go to Start
2. Select Programs
3. Choose Network Associates
4. Select VirusScan Console
5. Right Click on "VShield" icon
6. Click on "Properties"
7. Choose "Download Scan" and then click on "Properties"
8. You will be prompted to enter a valid password.
9. Enter any random password and VirusScan will return an error message (See Figure 26), then click on "Ok" and see number 11.
10. Don't enter any password and click on "Cancel".
11. The VirusScan will let you view the properties of "Download Scan" without being able to do any changes. (See Figure 27)

Notice: the Download Scan properties will view all the options grayed out, which means that you will not be able to do any changes. Just viewing mode.

Figure 26: Download Scan Properties (Invalid Password)

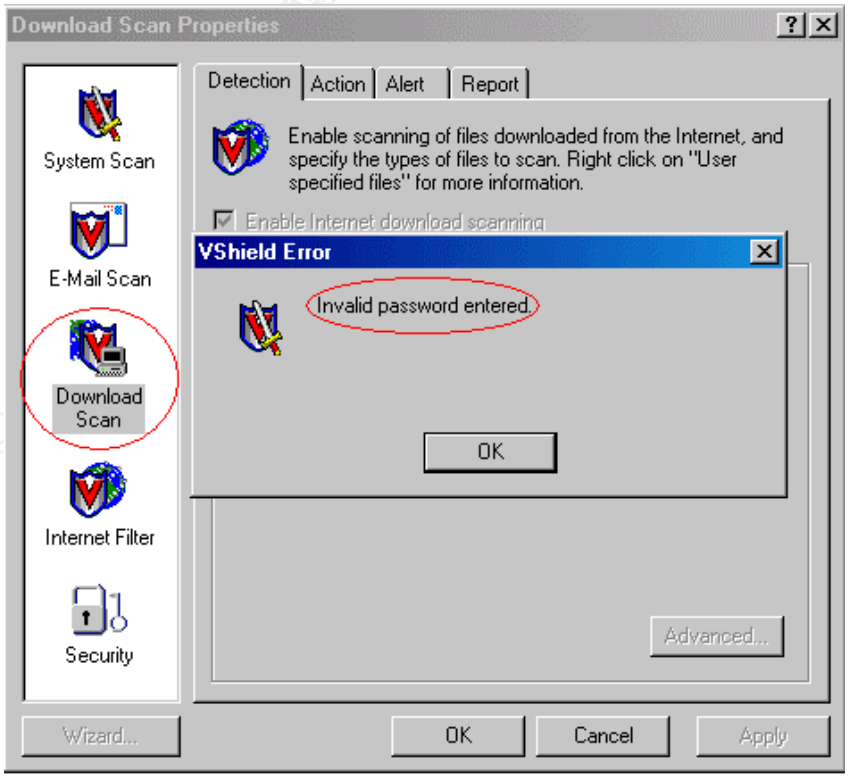
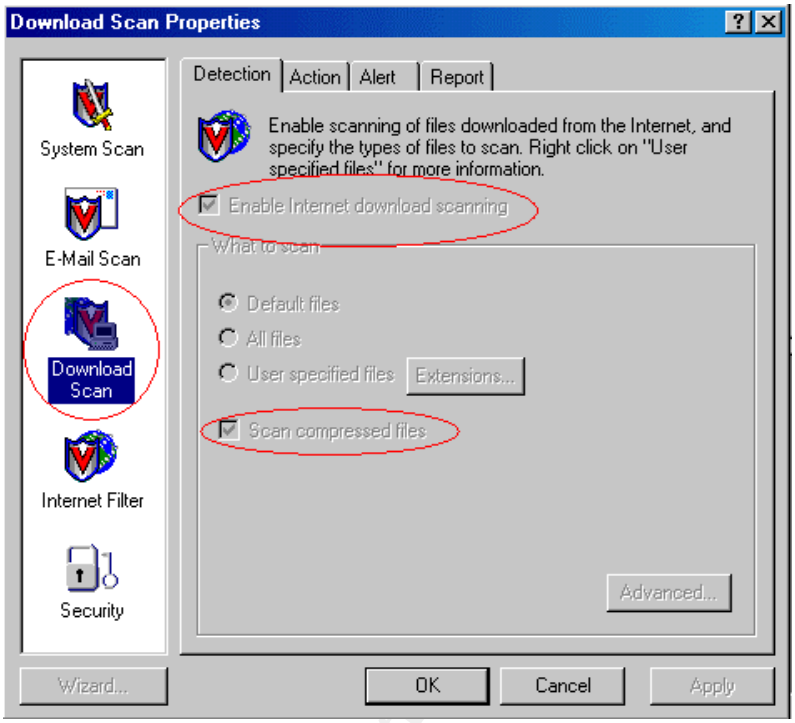


Figure 27: Download Scan Properties (Options Grayed)



Item Number 8: Verify that System Scan is password protected ☑

Compliance: Pass

Stimulus/Response:

1. Go to Start
2. Select Programs
3. Choose Network Associates
4. Select VirusScan Console
5. Right Click on "VShield" icon
6. Click on "Properties"
7. Choose "System Scan" and then click on "Properties"
8. You will be prompted to enter a valid password.
9. Enter any random password and VirusScan will return an error message (See Figure 28), then click on "Ok" and see number 11.
10. Don't enter any password and click on "Cancel".
11. The VirusScan will let you view the properties of "System Scan" without being able to do any changes. (See Figure 29)

Notice: the System Scan properties will view all the options grayed out, which means that you will not be able to do any changes. Just viewing mode.

Figure 28: System Scan Properties (Invalid Password)

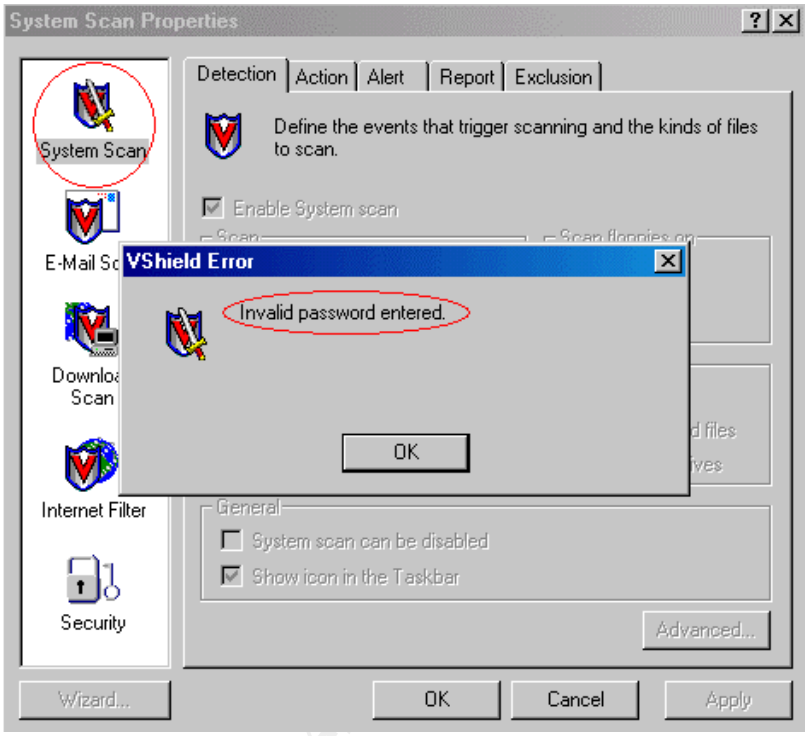
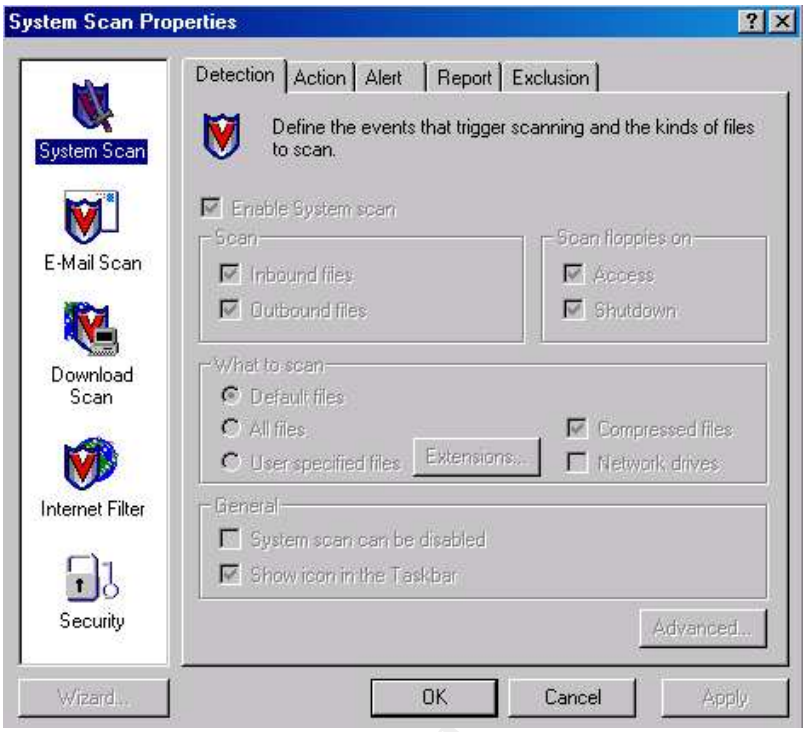


Figure 29: System Scan Properties (Options Grayed)



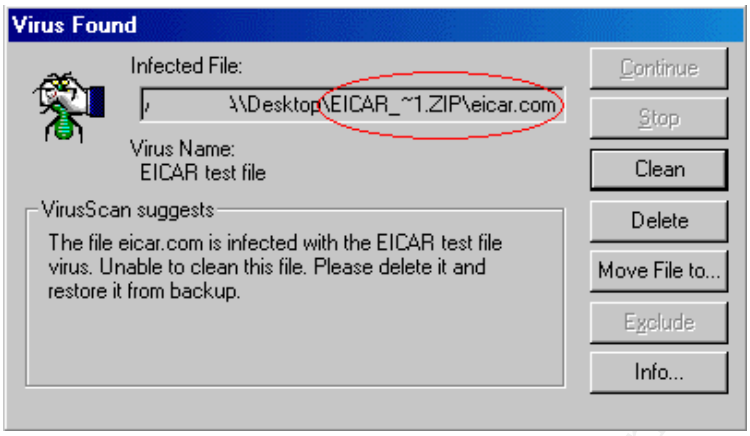
Item Number 9: Verify that VirusScan scans compressed files ☑

Compliance: Pass

Stimulus/Response:

1. Download Eicar_com.zip from http://www.eicar.org/anti_virus_test_file.htm and save it on the computer.
2. Locate the file and right click on it
3. Select to "Scan for Viruses"
4. The VirusScan detects the infected test file and the user is prompted for an action. See Figure 30

Figure 30: Virus Found (Compressed Files)



Item Number 10: Verify that the user does not have the option to "Continue scan" or "Stop Scan" ☑

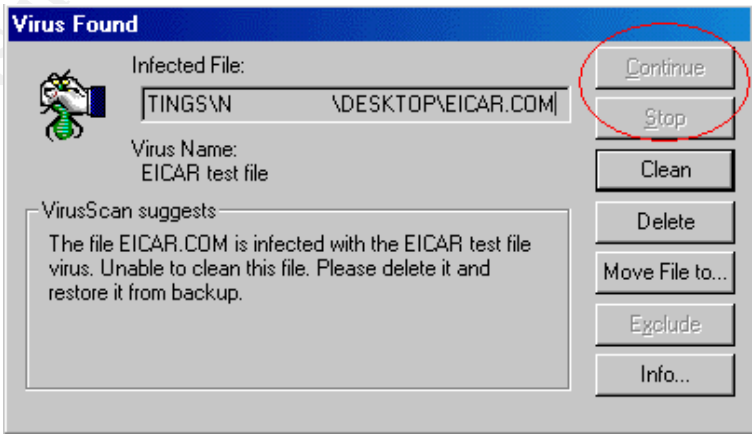
Compliance: Pass

Stimulus/Response:

1. Download EICAR.com
2. Save the file to the C: drive.
3. Right click on the file name.
4. Select "Scan for Viruses", and then click on "Scan Now".
5. The VirusScan will detect the infected file and will prompt the user for actions with the exception of “continue” or “stop” action. See Figure 31

Notice that continue and stop scan are not viewed as choices for the user.

Figure 31: Virus Found (Action)



Part 4 - Audit Report

Executive Summary

The scope was to audit McAfee VirusScan 4.5.1 SP1 installed on Windows 2000 Professional Operating System with Service Pack 4. The system that was audited was an employee's desktop computer. The target was to conduct a risk analysis, check the configuration of the system, test the options in the VirusScan, and verify the functionality of the Scanning abilities of the VirusScan. In addition, the audit focused on the protection of the configurations and settings of the VirusScan and verified that there are controls in place to protect these options and configurations from being disabled or changed by the user.

The audit scope was achieved and accomplished and below is the detailed audit findings and recommendations to increase the security of the company. In addition, the recommendations will add an extra layer of protection to the major asset of the corporation. The major asset of the corporation is the data.

Audit Findings

The summary of the findings based on the compliance is listed in the table below. In addition, the details of the tests are explained below.

Pass	Compliance Status
Verify that Download Scan is enabled.	Pass
Verify that System Scan is enabled. (Fail)	Fail
Verify that VirusScan Scans Floppy Disks (Fail)	Fail
Verify that VirusScan scans compressed files	Pass
Verify that Schedule and Configure of "AutoUpgrade" is password protected	Pass
Verify that Schedule and Configure of "AutoUpdate" is password protected	Pass
Verify that "Scan my Computer" is password protected	Pass
Verify that Download Scan is password protected	Pass
Verify that System Scan is password protected	Pass
Verify that the user does not have the option to "Continue scan" or "Stop Scan"	Pass

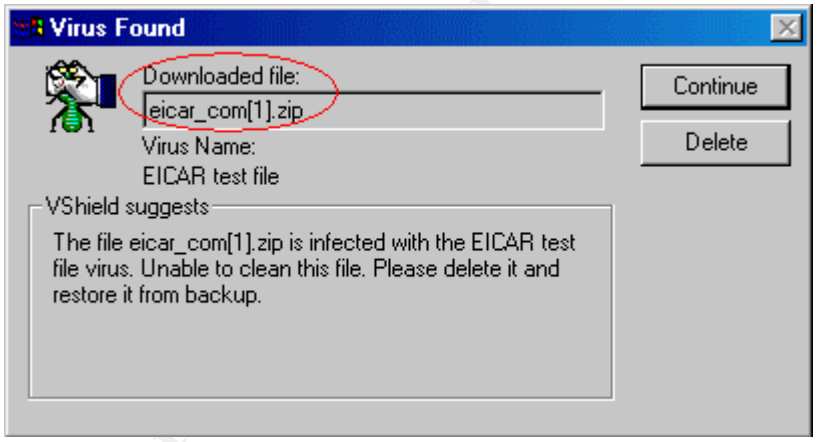
Item: Verify that Download Scan is enabled

This test was conducted on one of the company's desktops and it was done through downloading EICAR test file that is detected by the VirusScan as a test Virus. This test Virus does not cause any damage, it was purely designed to check the functionality of the different Anti-Virus software.

The audit item passed in this test, since the VirusScan detected that I am downloading a "Virus" and asked for action. Figure 32 shows the screenshot of the response from the VirusScan.

Risk: destruction of data (High), due to the fact that downloading infected files from the Internet causes malicious software to exist in the employee's computer and then can be distributed to the other computers within the network or to customers of the company.

Figure 32. Evidence 1



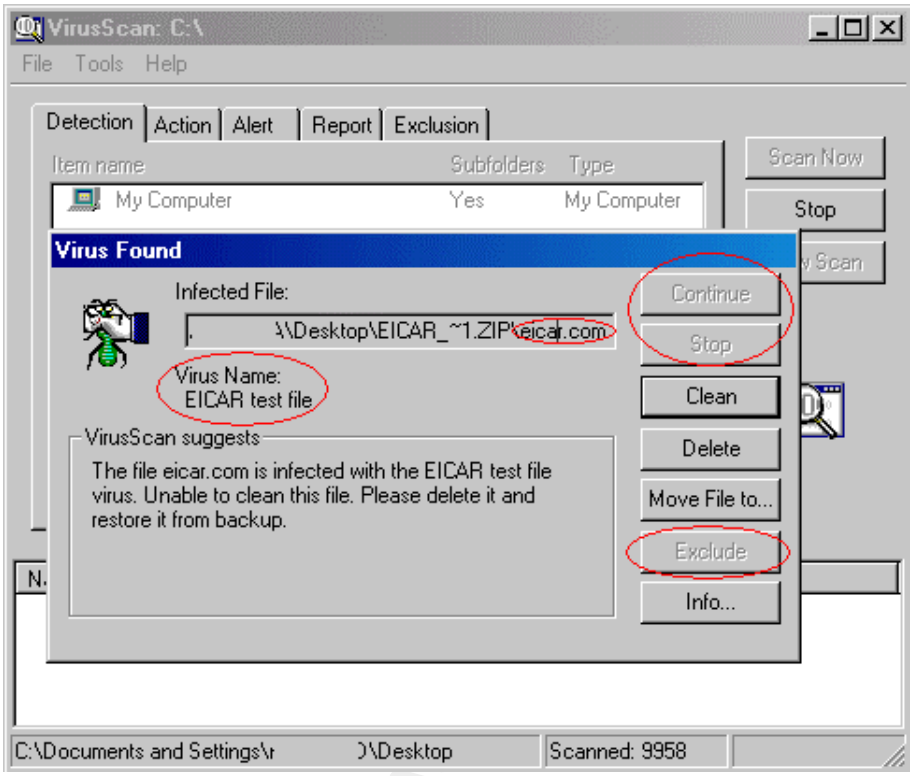
Item: Verify that System Scan is enabled.

The item of verifying the system scan was done through downloading EICAR test file and saving it on the desktop, and then noticing if the VirusScan detects that an infected file was residing on the desktop system.

The audit item failed in this test, since the VirusScan did not detect that the EICAR file was stored on the desktop system. The VirusScan detected the file after initiating the VirusScan scanning activity manually.

Risk: not detecting an infected files or folder (High), because if the system scan is not enabled that indicate that the computer is not scanning files residing on the system constantly, which means that any malicious software could be residing on the computer without being detected.

Figure 33. Evidence 2



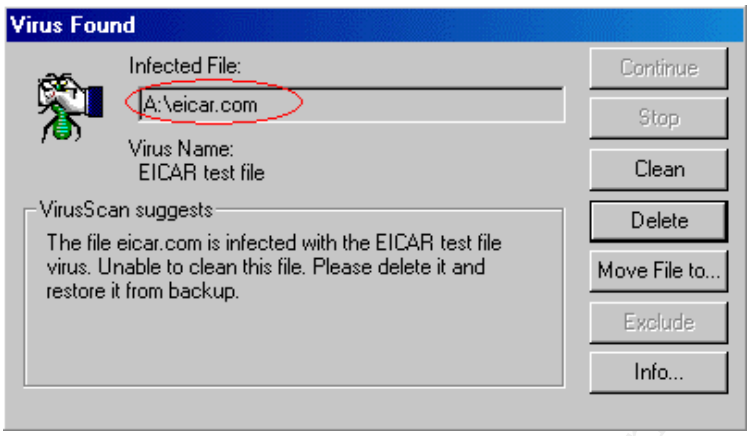
Item: Verify that VirusScan Scans Floppy Disks

Verifying the VirusScan option of scanning the contents of the Floppy disk, was a major and necessary part of the Audit tests. The Floppy disk had an EICAR Virus test file contained in it for the purpose of testing. The floppy disk was inserted to the desktop and tried to access the contents of the Floppy disk, but the VirusScan didn't detect that I am inserting a floppy disk that is "infected". Although, the VirusScan detected the EICAR virus test file by manually scanning the floppy disk's contents, the checklist item failed. Since the detection was not automatic, the checklist item of verifying the scanning of the floppy disk, failed.

Risk: distribute the infection from Floppy Disk to computers connected to the network (High), because all the corporate computers have Floppy Disks and they might be carrying infected files that can be transferred to the network and other computers in the company if the VirusScan does not scan Floppy Disks when inserted or a shutdown is taking place.

Figure 34 shows the detection of the EICAR virus test file after the manual scan was simulated.

Figure 34. Evidence 3

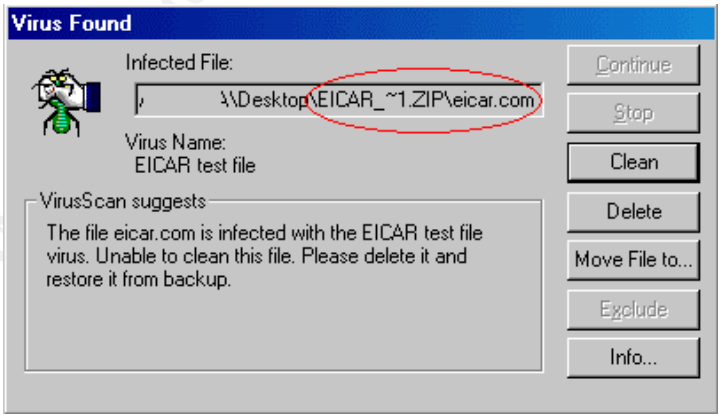


Item: Verify that VirusScan scans compressed files

The scan targeted testing the corporate VirusScan for the feature of scanning compressed files such as zipped file. The EICAR test virus has a compressed version to be able to evaluate the effectiveness of the Anti-Virus software. During the audit tests, I downloaded a compressed EICAR file that stimulated the VirusScan and fortunately enough the VirusScan detected that I am download an infected file and prompted me for the appropriate action.

Risk: users disabling of scanning of compressed files and VirusScan not detecting infected compressed file (High), due to that compressed files can contain infections.

Figure 35. Evidence 4



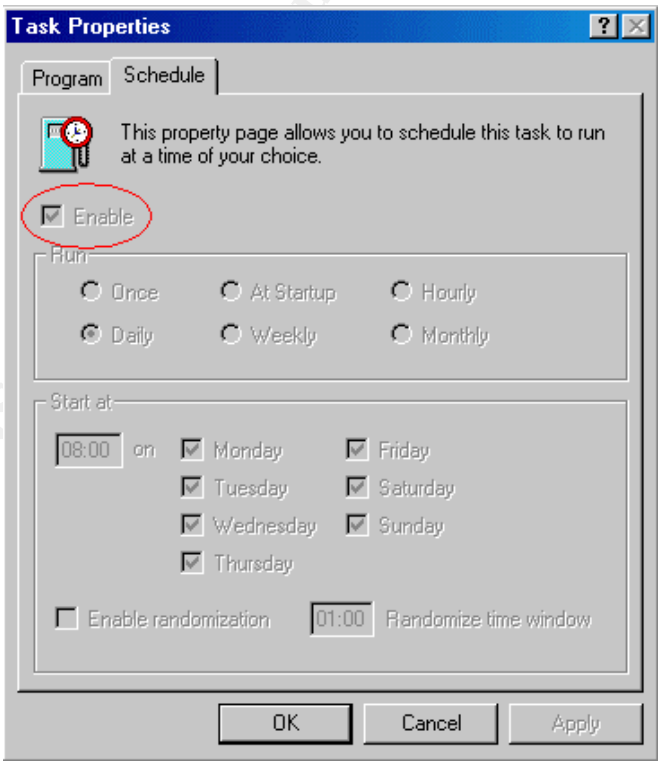
Item: Verify that Schedule and Configure of “AutoUpgrade” is password protected

The item checks that the user can’t change the configuration of the autoupgrade option and to verify that the option is password protected. The simulation for the test, was by typing incorrect password or leaving the password field blank.

Risk: not having upgrades of the VirusScan that Network Associates issued (Medium), the danger of being able to change the schedule or configuration of the "autoupgrade" is that the user can disable upgrading the VirusScan which means not being able to downloading and installing new program files, including new scan engine versions, service packs, and hot fixes files.

This item in the checklist passed since the user without valid password was able to enter the configuration and schedule screen but can’t change any options. Figure 36 shows the schedule screen and all the options are grayed out which means the user can’t change any option within this section. This screen shows the option is for viewing only without making any changes.

Figure 36. Evidence 5



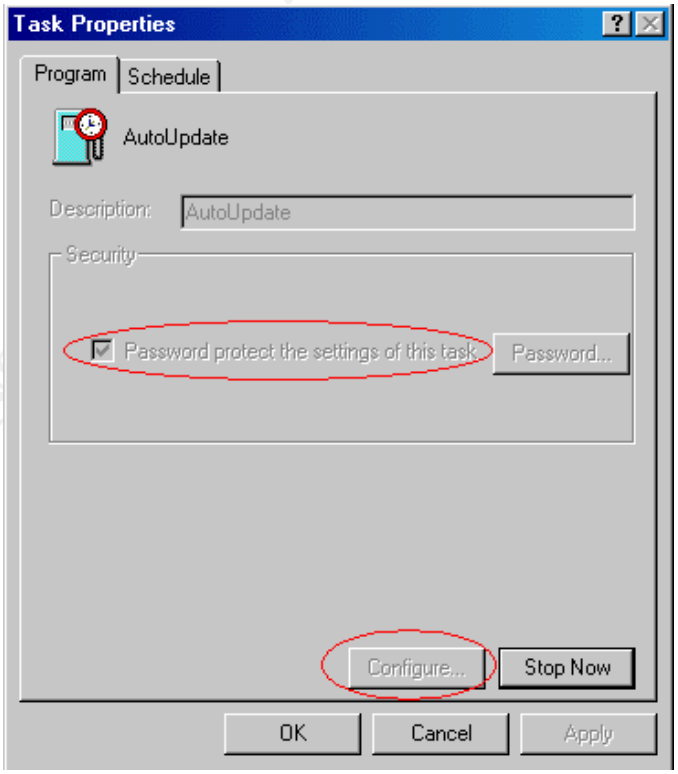
Item: Verify that Schedule and Configure of “AutoUpdate” is password protected

The item checks that the user can’t change the configuration of the autoupdate option and to verify that the option is password protected. The simulation for the test, was by typing incorrect password or leaving the password field blank.

Risk: out of dates virus signatures (High), due to the fact that disabling Autoupdate or changing it's configuration will cause great danger to the computer since Autoupdate downloads and installs the new virus definitions (.DAT) files to the VirusScan software which protects the computer from new viruses and other malicious software.

This item in the checklist passed since the user without valid password was able to enter the configuration and schedule screen but can’t change any options. Figure 37 shows the schedule screen and all the options are grayed out which means the user can’t change any option within this section. This screen shows the option is for viewing only without making any changes and indicates that the option is password protected as well.

Figure 37. Evidence 6



Item: Verify that "Scan my Computer" is password protected

The item checks that the user can't change the configuration of the "Scan my computer" option and to verify that the option is password protected. The simulation for the test was by typing incorrect password or leaving the password field blank.

Risk: users disabling scanning of compressed files or heuristic scanning or changing any of the "Scan my Computer" configuration (High), because if the user changes the configuration of "scan my computer" then can disable scanning of compressed files, and disable heuristic scanning of programs and files, which will cause the VirusScan not able to detect infected compressed files or macros.

This item in the checklist passed since the user without valid password was able to enter the configuration and schedule screen but can't change any options. Figure 39 shows the schedule screen and all the options are grayed out which means the user can't change any option within this section. This screen shows the option is for viewing only without making any changes. Figure 38 shows the prompt message after entering an invalid password.

Figure 38. Evidence 7

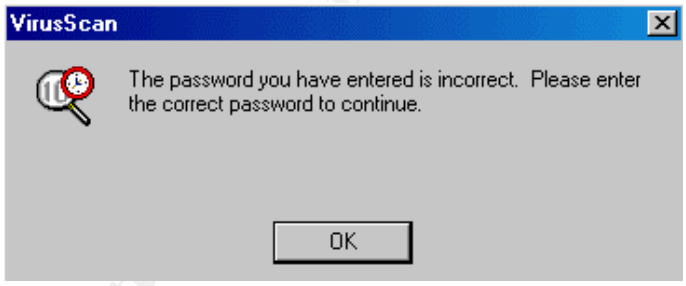
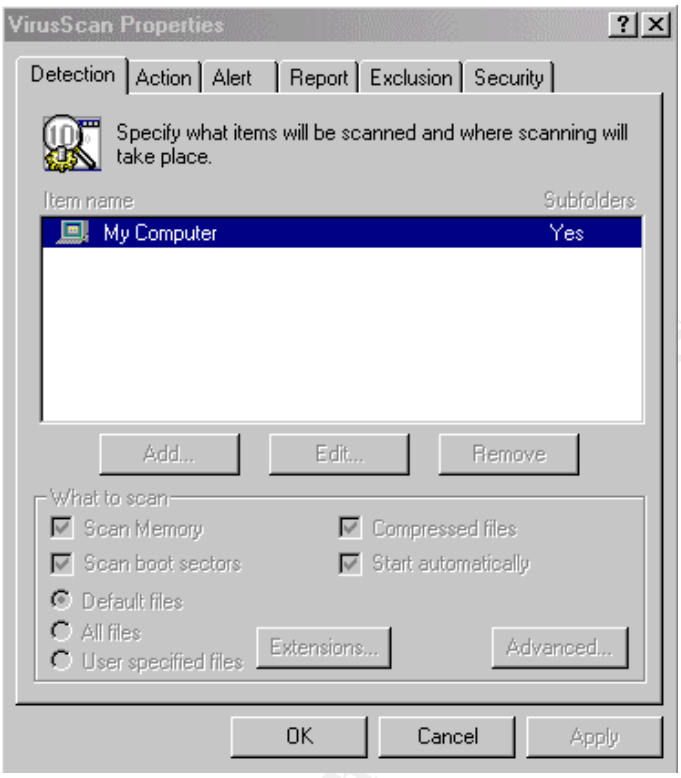


Figure 39. Evidence 8



Item: Verify that Download Scan is password protected

This item's aim was to verify the protection of the download scan configuration screen. The audit was conducted through entering an invalid password for the download scan settings area. The VirusScan enabled the viewing of the configuration screen and disallowed the modification of any option within the configuration screen.

Risk: users disabling the feature of scanning downloaded files (High), due to that disabling download scan will cause the VirusScan not able to scan files while downloading them from the Internet that could be infected.

The download scan option protects the computer from downloading infected files that contain any type of malicious software.

Figure 40. Evidence 9

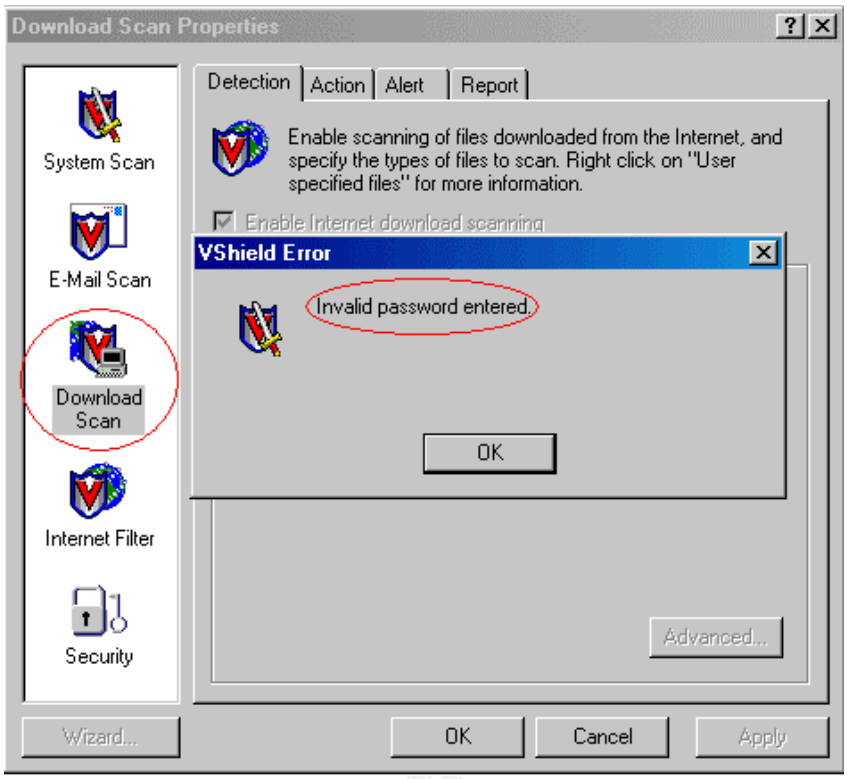
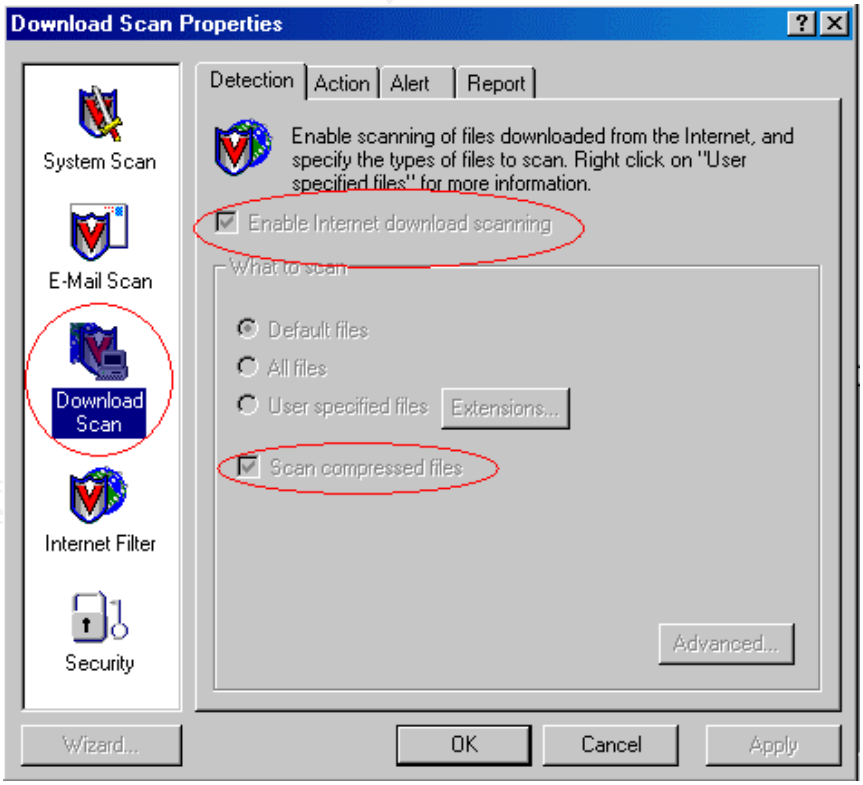


Figure 41. Evidence 10



Item: Verify that System Scan is password protected

This item's target was to verify the protection of the system scan configuration mode. The stimulus was by entering an invalid password (Figure 42). The VirusScan prompted for entering a correct password and by clicking "ok" the user was able to view only the settings without making any changes to the configuration tab (Figure 43).

Risk: users misconfiguring system scan by disabling it from scanning (Medium), due to that disabling system scan will cause any infection not to be found if the user changes the configuration of the System Scan without password.

The system scan is very important and critical because it is considered the live scan of the desktop's system files.

Figure 42. Evidence 11

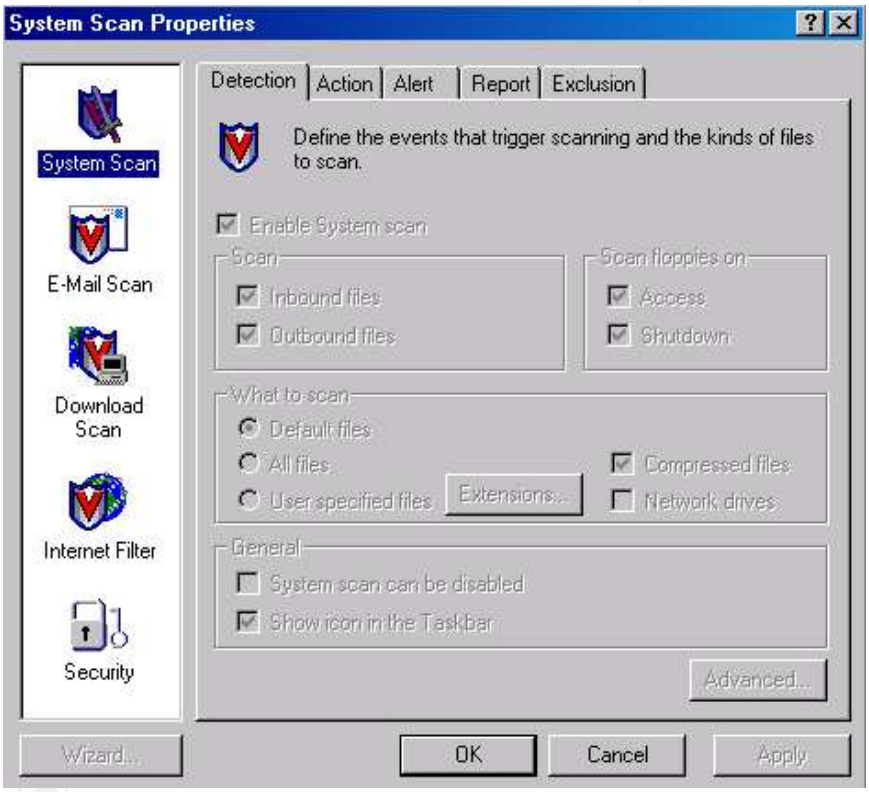
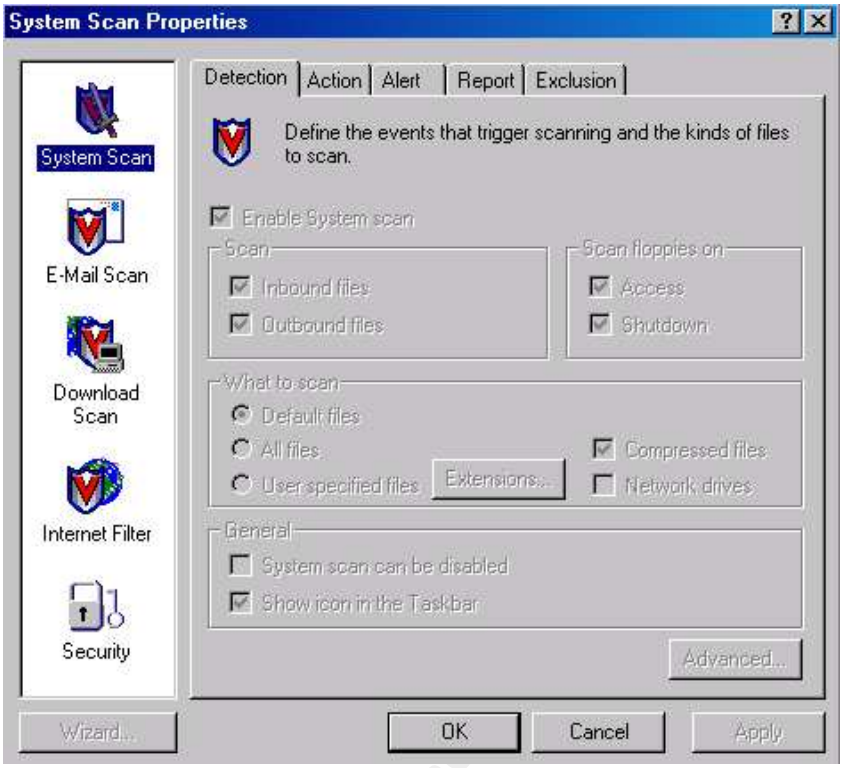


Figure 43. Evidence 12



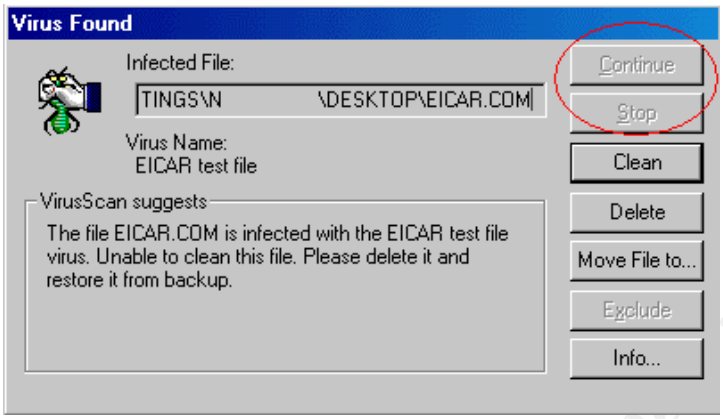
Item: Verify that the user does not have the option to "Continue scan" or "Stop Scan"

The checklist item passed because the VirusScan detected the EICAR.COM file and prompted the user for all options with the exception of “Stop” and “Continue” scanning options. See Figure 44

Risk: user continue or stop scanning selected as action and infection remains on the computer (High), because continuing or stopping the scan does not clean, delete the infected files which means that the malicious software will be residing the system.

The importance of verifying the option of Continue and stop scan, is that if a virus or any infected file was found, the user should not be able to continue the scan without curing the infected file. The stop scan is another feature that gives the user the option to stop the scanning without any proper action dealing with the infected file.

Figure 44. Evidence 13



Audit Recommendations

Recommendations

The audit results and finding were clearly explained previous, and the risks were identified for each checklist item. As a result, I would like to list the following recommendations that would increase the security of the company and enhance the current protection measures. The major risk that is threatening the computer world, and especially the computers that are connected to the Internet cloud is the fear of being infected by any type of malicious software that degrades the confidentiality, integrity, and availability of the data.

The first and most important recommendation is to have a security awareness program of the importance of updating the Anti-Virus definitions and scanning the desktop on daily basis. Furthermore, explaining to the employees the symptoms of being infected by malicious software. Educate users to scan any floppy disk before accessing the floppy disk or copying the files to the corporate computers.

Second, deploy anti-virus software that can be supervised and monitored by the administrator. In addition the administrator should be trained to check the logs and centrally manage the Anti Virus software including alerts, update, and upgrades.

Third, install firewall on the network to insure the security of the employees and their data or purchase software that has new Anti-Virus software with personal firewall included with the software.

Finally, evaluate and test different Anti-Virus software to find software that immediately scans and detect infected files or folders on the system or contained in Floppy disks.

Cost

The main fix that can be applied to cure most of the weaknesses in the current security state is to upgrade the Anti-Virus software. The cost will be to purchase a new version of the Anti-Virus software for the corporate edition. The recommended software for upgrade is McAfee Active VirusScan Suite Small Business Edition. The price per seat for users between 51 and 100 is $32.56 per seat; the total software price for approximately purchasing 70 licenses is equal to $2279.2. System performance will be constant as with the current Anti-Virus software. The man-hours involved will be approximately between 20 - 25 hours doing the installation and securely configuration the Anti Virus Software.

In addition, another recommendation is to install a firewall in the network or install personal firewalls on each desktop. I would recommend both to insure that the security of the network is guaranteed with the layered security approach. The installation and configuration of the firewall (personal) will required approximately 15 hours, while installation and configuration of network based firewall will approximately require 2-4 hours depending on the configuration.

Compensating Controls

The first control is to implement a security policy for the company. The security policy should include Anti-Virus policy, computer usage, Internet usage, and E-Mail usage policy. The security officer of the corporate and the coordination of the Professional Services department and other department heads should write the policy and also the process owners should be involved in the process of writing the company's security policy.

The second Compensating controls is to aware the staff of the importance of anti-virus and how bad the malicious software can cause to the organization and it's reputation in the market. Also, having presentations and discussions of the benefits of running Anti-Virus scan daily and keeping the system updated with patches and updates.

The third control that can be freely available is to install a personal firewall on the individual computers to increase the security of the computers and limit the infected computers from distributing over the network.

The last control is that the company can have a strict procedure that the administrator has to review the settings, configurations, and logs of the VirusScan weekly at least and make sure that the updates and upgrades are the latest and scanning has been taking place regularly and the computers are in clean status.

Appendix A: Table of Figures