Auditing LANguard File Integrity Checker V 1.0: An Auditor's Perspective

David Pierce

October 2002
SANS GSNA Practical v 2.0

Table of Contents

Assignment 1 - Research in Audit, Measurement Practice, and Control

Introduction

Host based file integrity applications play a detective role in computer security. The purpose of file integrity verification applications is to notify the system administrator of added, deleted, or modified files within the organization's computer systems. Files that should be selected for verification typically do not change under normal conditions. These types of files include executables, dynamic link libraries, system files, device driver files, etc. File integrity applications work by creating a cryptographic baseline signature or 'hash' value of each file that has been selected for verification. Each time the application runs, a new hash value is generated for each selected file. This new value is then compared to the baseline. If the two values do not match, a notification is sent to the administrator to alert them that files have changed and should be investigated for possible malicious activity. File integrity checking should not be the only means of protection; it should be the last-line of a multi-layered defense strategy (Rauch 1).

I am auditing LANguard File Integrity Checker version 1.0 on a Windows 2000 Professional workstation with service pack 3 installed. The workstation has a 300 MHz Pentium II processor and 196 MB of RAM. This application performs a detective role to determine the integrity of files.

The primary goal of this audit is to ensure that company policies/procedures regarding system software change control are being followed. The secondary goal is to validate vendor claims and to ensure that the file integrity application maintains availability, integrity, and confidentially.

The scope of this audit is limited to the specified application. Assumptions are that the computers are properly baselined[1] (Hoelzer 1-3) and securely configured[2]. Baselineing the computers and securing the operating system is outside the scope of this paper, however, application specific security will be discussed and tested. All tests will be conducted in a controlled lab environment to protect the production systems. The lab computer is configured the same as the production computers. All computers are Windows 2000 based with service pack 3 installed.

LANguard File Integrity Checker (version 1.0) is a freeware product that provides host based intrusion detection, specifically file integrity validation. This application only runs on Windows NT/2000/XP. LANguard File Integrity Checker creates a MD5 signature of selected files (Ref Figure 1) and stores this information in a Microsoft Access

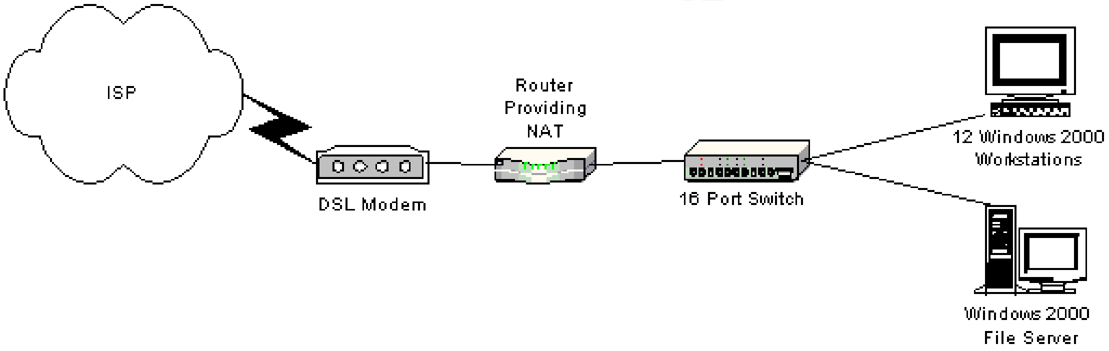
[1] Baselineing refers to having a known good state; administrators must know what is on their system and how it is configured (Hoelzer 1-3).

[2] All security patches installed, unused accounts removed, and unnecessary services removed (Kolde 1-12).

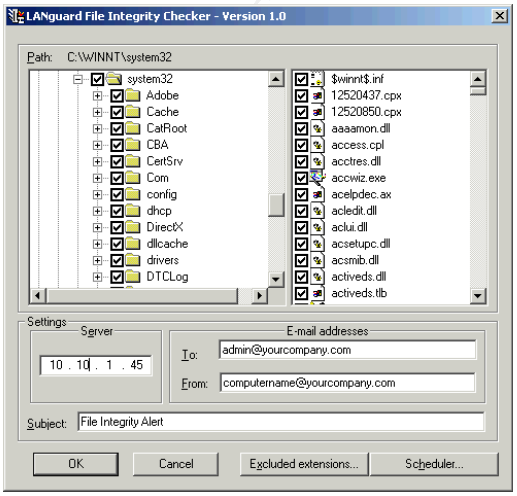
database. It is capable of scheduled operations, which helps to automate the system administrators tasks (Ref. Figure 2). It detects and reports files added, deleted, or modified (LANguard File Integrity Checker 1). The reason for selecting this application was that the application is free for download, and easy to install and configure. Small to mid sized businesses may not have the financial resources or expertise available for other commercial applications of this type.

System Overview

The system consists of a business class DSL cable modem connection to an ISP. All of the computers are Windows 2000 with service pack 3 installed. A router provides Network Address Translation (NAT) to private IP addresses and feeds a 16-port switch. There are 12 workstations and one file server. The file server supports a commercial accounting application.



Application Interfaces



Path: C:\WINNT\system32

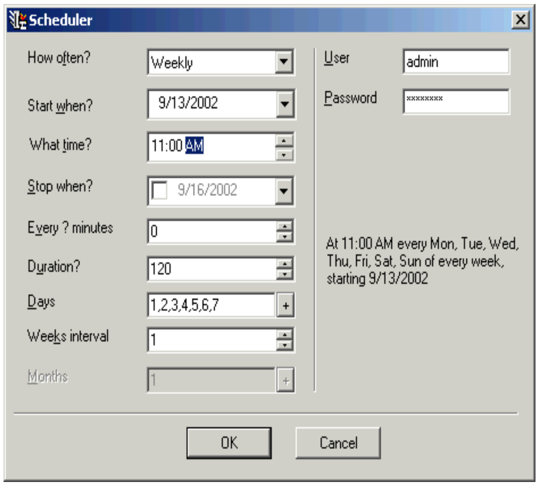
Server: 10 . 10 . 1 . 45

To: admin@yourcompany.com

From: computername@yourcompany.com

Subject: File Integrity Alert

Figure 1 Configuration Interface



Scheduler

How often? Weekly

Start when? 9/13/2002

What time? 11:00 AM

Stop when? ☐ 9/16/2002

Every ? minutes 0

Duration? 120

Days 1,2,3,4,5,6,7

Weeks interval 1

Months 1

User admin

Password ********

At 11:00 AM every Mon, Tue, Wed, Thu, Fri, Sat, Sun of every week, starting 9/13/2002

Figure 2 Scheduler Interface

Evaluate the risk to the system.

All computing environment face many risks and threats. External attackers, internal employees, natural disasters, and power outages are just a few. External threats can range from port scans to system compromise. Internal threats can range from employees introducing malicious code (viruses) to installing software tools in an attempt to gain unauthorized access to company sensitive information. A secondary benefit of this application is the reporting of when a baseline has changed.

The likelihood of these risks will depend on whether the threat is from external attackers or internal employees. The risk of an external attacker gaining access to the computer system is moderate to low because of the router that provides network address translation functionality. The risk of internal employees is high because they are already inside the defensive mechanisms.

The consequences of both external and internal threats are the same and can range from system compromise, theft of sensitive data, the company's computer system being used as a relay for other illegal computer activities, or software licensing violations. The following table describes the risks to the system, the likelihood of the event occurring, and the impact to the organization/computer system.

Risk	Likelihood	Impact
Non existent or unclear computer security policy	In a small to mid sized company, a computer security policy may not exist or is not clear on what the policy is meant to achieve.	If a policy does not exist or is poorly written, the company will not have control over it's IT resources

Improper segregation of duties	In a small to mid sized company with limited computer security experience, segregation of duties may not be implemented	Improper segregation of duties can range from misuse of resources to theft of company sensitive information/assets.
Service visible to the network	Internal: Medium External: Low	The computer may be compromised by an exploit against the service, or at least the application may not work as expected
Improper configuration	Medium	If the application is improperly configured, it may not check critical files or send the report.
Patches not installed	Internal: Medium External: Low	If there are known vulnerabilities and patches are not installed the likelihood and impact of a compromise will be high.
Unauthorized software added	Internal: High External: Low	The impact can range from license violations to complete compromise of the system.
Critical files modified or deleted.	Internal: High External: Low	Unauthorized file content modification could be an indication of attacker activity

Table 1 System Risks

What is the current state of practice and how can they be improved

I have searched www.google.com, www.altavista.com, www.yahoo.com, and at www.auditnet.org for file integrity audit procedures/checklists. There are other change control checklists but the subject matter is more inline with computer software source code, not an application of this type. After determining that there are no guidelines or checklists for auditing this type of application, I have used the information from CobiT and FISCAM as the basis for this audit checklist.

Assignment 2 –Create an Audit Checklist

The following checklists have been developed to measure compliance for this audit. Each control objectives is designed to be as objective and verifiable as possible. Application input controls are discussed in tests 8, 11, 12 and 22-24. Processing controls are discussed in tests 7, 13-21, and 25. Application output control is discussed in test 6. A flow chart for this process is located in appendix A.

Risk Rating

Risk rating is a quantifiable measurement of the consequence if the control objective is not met. The risk rating allows management to prioritize deficiencies. High priority issues should be addressed first.

Risk Rating = Likelihood X Consequence

Likelihood	**Consequence**
1 = Unlikely	**1 = Minor impact**
2 = Possible	**2 = Major Impact**
3 = Probable	**3 = Critical Impact**

Risk Rating

1 or 2	=	Low priority
3 or 4	=	Medium priority action
6 or 9	=	High priority action

Policy/Procedure Review

Documentation review is the first step to determining what the rules are in the organization and who is assigned what responsibilities. Among the policies and procedures that require review are system software change controls and incident response. These policies/procedures should exist and be current.

Test Item 1 Documentation Review

Control Objective	Detailed Policy/Procedure review
Risk	Policies and procedures are the rules that all employees must follow. Not having computer security policies/procedures prohibits the company from having control over their resources and can leave the company vulnerable to unauthorized: computer usage, application installation, theft of company sensitive information, and confusion during an incident.

Risk Rating	Likelihood 3 Consequence 3 = High priority action
Reference	CobiT
Test	Review company computer security policies/procedures including, but not limited to, overall security policy, change management, and incident response for evidence of: • Confidentially, Integrity, Availability, Accountability statements Detailed change control and incident response procedures including: • On what basis changes should be approved • Who approves changes • Clearly stated roles and responsibilities • What the response is to unauthorized changes
Result	
Compliance	Compliance will be determined by how well documented the policies/procedures are.
Objective Subjective	Subjective
Pass/Fail	

Test Item 2 Organizational review

Control Objective	Ensure proper segregation of duties
Risk	Improper segregation of duties can allow a single individual to take advantage of company resources for personal gain or to cover up inappropriate activities. These activities can range from misuse of resources to theft of company sensitive information/assets.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Review the companies organizational structure and job descriptions for proper segregation of duties.
Result	
Compliance	Compliance will be determined by how well documented the policies/procedures are.
Objective Subjective	Subjective
Pass/Fail	

Known Deficiency Research

Known deficiencies need to be identified in order to determine what the risks are to the version being audited.

Test Item 3 Application Patches

Control Objective	Determine if the product has any known deficiencies that adversely impact the application or security.
Risk	Product deficiencies could give an attacker the opportunity for exploit.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Visit the vendor website http://www.gfi.com/ and look for patches pertaining to LANguard File Integrity Checker. Go to the ICAT website (http://icat.nist.gov/icat.cfm) and look for vendor (GFI) and product (LANguard File Integrity Checker) vulnerabilities. If there are any patches or known weaknesses, ensure that the latest version is installed.
Result	
Compliance	The results of this test are binary. Either there are known weaknesses, or not. If there are known weakness the latest version should be installed. The version number is displayed on the configuration interface. To bring the application interface up, go to Start ->Programs->LANguard File Integrity Checker Configuration.
Objective Subjective	Objective
Pass/Fail	

Identify All Access Paths

All access paths should be identified in order to determine what potential attackers could see.

Test Item 4 Network Path

Control Objective	Evaluate controls over external access
Risk	Network visible services are an attackers first “look” at the system. If the file integrity service is visible, it could be vulnerable to a remote attack if there is an exploit available. If an attack is successful, the computer may become compromised, the attacker may be able to run code of his/her choice, or at least the application may not work as expected.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM, Vendor documentation Vendor documentation states that a service is installed (Cfservice) but does not indicate that it is network accessible.
Test	Utilizing a port scanner, scan all ports (65535 TCP/UDP) from another machine to determine if the service is visible from the network. The results should not reveal the “Cfservice” is running.

Result	
Compliance	The results of this test are binary. The Cfservice should not be visible from the network.
Objective Subjective	Objective
Pass/Fail	

Test Item 5 Host Path

Control Objective	Identify all access paths
Risk	There should not be any services running under the application service (Cfservice). If there is then the other service should be investigated for possible malicious activity. The vendor information does not indicate that any other service is running under the Cfservice.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Using the application Tlist.exe from the Microsoft Windows 2000 Installation CD (This application must be extracted prior to use. Navigate to Support\Tools folder on the Windows 2000 installation CD; extract the Tlist.exe utility from the Support.cab file). From the command prompt, change directories to the location that tlist.exe was extracted to and type the command Tlist –s. The output from Tlist.exe will show what services are running under each process. The –s option shows services active for each process in a tree view. For more information see http://is-it-true.org/nt/atips/atips301.shtml
Result	
Compliance	The results of this test are binary. No other services should be running under the Cfservice process.
Objective Subjective	Objective
Pass/Fail	

Data Integrity

Data that is sent from one computer to another is subject to interception and manipulation. Data integrity ensures that the information that is received is exactly the information that was sent without manipulation.

Test Item 6 Report Protection

Control Objective	Protection of sensitive messages.

Risk	If the report is intercepted and manipulated in-transit and there is no mechanism to detect this type of activity, the system administrator may not receive an accurate report. This could significantly impact the decision process.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Examine the report for evidence of a digital signature.
Result	
Compliance	The results of this test are binary. The report should be digitally signed to detect in-transit manipulation.
Objective Subjective	Objective
Pass/Fail	

Test Item 7 Cryptographic Signature

Control Objective	Verify that a cryptographic file integrity signature is created
Risk	If the file integrity signature is not encrypted, i.e. MD5, SHA1 etc. an attacker could alter the signature to hide their activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	CobiT
Test	Have the administrator 1. Open the Cfdata.mdb database 2. Open the "old_Data" table and verify that a hash value for the files has been created.
Result	
Compliance	The results of this test are binary. There should be a hash value for each file in the database
Objective Subjective	Objective
Pass/Fail	

Test Item 8 Full File Name

Control Objective	Verify that the full filename is reported
Risk	It is imperative that the application reports the full file name. If the full file name is not reported, it may be very difficult to determine exactly which file was altered.
Risk Rating	Likelihood 3 Consequence 2 = High priority action
Reference	CobiT

Test	Windows 2000 has a maximum of 215 characters for a file name. Create a test file with 215 characters. Run the application and verify that the full file name has been reported.
Result	
Compliance	The results of this test are binary. The application should detect and report the full file name.
Objective Subjective	Objective
Pass/Fail	

Least Privilege

Least privilege is the control that ensures only persons that require access to sensitive applications/utilities have that access. Access by all other persons should be denied.

Test Item 9 Service Security

Control Objective	Ensure least privilege.
Risk	If non-administrators have access to the application or its underlying service, proper operation of the application cannot be ensured. It would be possible for internal users to hide their activities.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Log on with user permissions and attempt to stop the application by 1. Start the task manager by pressing ctrl + alt + del. 2. Select Task manager 3. Select the Processes tab 4. Select Cfservice.exe 5. Click End Process 6. Acknowledge the task manager warning by clicking yes
Result	
Compliance	The results of this test are binary. After clicking yes at the task manager warning, There should be a message that states, “Unable to terminate process access is denied”.
Objective Subjective	Objective
Pass/Fail	

Test Item 10 Protect Configuration Files

Control Objective	Configuration file protection
Risk	Without proper change control, the configuration files could be modified preventing the application from functioning or processing irregularities could be introduced.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Log on to the computer with user permissions and attempt to modify the initialization configuration file located at C:\Program Files\LANguard File Integrity Checker\Data\CFData.ini by adding three (3) characters to the end of the file.
Result	
Compliance	The results of this test are binary. Anyone without explicit authorization should not be able to modify the configuration or associated files.
Objective Subjective	Objective
Pass/Fail	

Test Item 11 Application Schedule

Control Objective	Determine scheduler controls and access authorizations.
Risk	If the users can access the schedule, they could modify it or disable the schedule completely. If the users did disable the schedule, the application would not run resulting in a high risk of unauthorized file modification.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Have the administrator use the built-in scheduler and schedule a file check with the administrator user ID and password. Have the administrator log out and have a non-privileged user log in. The scheduled task should complete. With the non-privileged user logged in, examine the task scheduler for the LANguard File Integrity Checker schedule. The scheduled job should not be visible.
Result	
Compliance	The results of this test are binary. The scheduled task should not be visible to the non-privileged user and the application should run as expected.
Objective Subjective	Objective
Pass/Fail	

Inappropriate/Unusual Activities Detected

This is what file integrity verification software is designed to do. If the application does not detect inappropriate/unusual activities, then the application fails to provide a useful function.

Test Item 12 Files Identified

Control Objective	All critical files are identified.
Risk	This type of application verifies the integrity of files. If critical files are not identified and monitored, the application will not provide information on the status of critical files
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Navigate to start->program files-> LANguard File Integrity Checker -> LANguard file integrity checker configuration. Review all files that have been selected. These should be files that are not expected to change.
Result	
Compliance	This is a subjective test but, selected files should include executables (.exe), dynamic link libraries (.dll), system files (.sys), device drivers (.vxd) etc…
Objective Subjective	Subjective
Pass/Fail	

Test Item 13 Addition of New Users

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report the addition of new users to the system
Risk	When adding a new user to the system, the SAM file will change and there should be an audit trail to determine if it was an authorized user or an attacker.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Have the system administrator add a new user to the system and run the application select start ->programs -> LANguard File Integrity Checker -> check now. Examine the output of the application for a modified SAM file.
Result	
Compliance	The results of this test are binary. The SAM file should show that it was modified.

Objective Subjective	Objective
Pass/Fail	

Test Item 14 Files Added

Control Objective	Inappropriate or unusual activities detected for files added.
Risk	This test is necessary to determine if an attacker has compromised the computer or if rouge software is added to the system.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Add a test file to the system and run the application. Examine the output report for the addition of the test file.
Result	
Compliance	The results of this test are binary. The report should show that a file was added to the system.
Objective Subjective	Objective
Pass/Fail	

Test Item 15 Files Deleted

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report files deleted
Risk	Files that have been deleted could be an indication that the system needs to be examined for attacker activity or malicious code.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Delete the test file that was added in the previous step and run the application. Examine the output for the deletion of the test file.
Result	
Compliance	The results of this test are binary. The report should show that the file was removed from the system.
Objective Subjective	Objective
Pass/Fail	

Test Item 16 Files Modified

Control Objective	Inappropriate or unusual activities detected for file content modification.
Risk	Unauthorized file content modification could be an indication of attacker activity.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Modify the content of a test file by adding three (3) characters and run the application. Examine the output for evidence of the test file modification.
Result	
Compliance	The results of this test are binary. The report should indicate that the file was modified.
Objective Subjective	Objective
Pass/Fail	

Test Item 17 File Attribute Change

Control Objective	Inappropriate or unusual activities detected. The application should detect and report file attribute changes (i.e.. Hidden, System, Read Only)
Risk	Attackers try to hide their tools. The application should detect these changes.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Utilizing the tool Properties Plus, change the attributes of three (3) test files to hidden, system, read only, and run the application. Examine the output for the attribute changes of the test files.
Result	
Compliance	The results of this test are binary. File attribute changes should be detected and reported.
Objective Subjective	Objective
Pass/Fail	

Test Item 18 File Date and Time Changes

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report file time and date changes
Risk	Attackers can alter file dates and times to conceal their activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action

Reference	FISCAM
Test	Utilizing the tool Properties Plus, Change the date on one of the test files and the time on another test file and run the application. Examine the output for the modification of dates and times of the test files.
Result	
Compliance	The results of this test are binary. The application should detect and report the time and date change if the test files.
Objective Subjective	Objective
Pass/Fail	

Test Item 19 Time and Date of File Change

Control Objective	Inappropriate or unusual activities detected. Does the application report the time and date of file changes.
Risk	Reporting the time and date of change is critical in determining when the activity took place. It is a step in reconstructing the attackers activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Modify one of the test files and run the application. Examine the output of the report for date and time of file change.
Result	
Compliance	The results of this test are binary. The report should indicate the time and date of the file change.
Objective Subjective	Objective
Pass/Fail	

Test Item 20 File Size Difference

Control Objective	Inappropriate or unusual activities detected. Does the application report before, after, and difference of file size.
Risk	This is necessary to determine if data was added or deleted. Configuration file alterations could lead to the masking of attacker activities.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM

Test	Modify two (2) test files. One to increase the size of the file by adding three characters. Modify the other test file to remove three characters. Run the application. Examine the output report for file size before, after, and difference on the test files that have been modified.
Result	
Compliance	The results of this test are binary. Before and after file size should be reported.
Objective Subjective	Objective
Pass/Fail	

Test Item 21 New Subdirectory

Control Objective	Inappropriate or unusual activities detected. Determine if the application will detect a newly created subdirectory.
Risk	Attackers typically add subdirectories to place their files.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Create a subdirectory by navigating to start ->programs->accessories-> windows explorer. Select the C drive and go to the menu, file->new folder. Run the application and examine the report to determine if the application detected the new subdirectory.
Result	
Compliance	The results of this test are binary. The application should detect and report that a new folder was added to the system.
Objective Subjective	Objective
Pass/Fail	

Validate Application

These tests are specific to the application.

Test Item 22 Non-SMTP Server Address

Control Objective	Validate application operation
Risk	Misconfiguration would prevent the application from sending the report. If the report cannot be sent, the system administrator will not be notified of changes.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT

Test	Enter an IP address that is not a SMTP server. This test will validate error messages indicating a misconfiguration. Ref Figure 1
Result	
Compliance	The results of this test are binary. There should be an error message indicating that the application cannot send the report.
Objective Subjective	Objective
Pass/Fail	

Test Item 23 File Exclusions

Control Objective	Validate application operation to determine if the list of excluded file extensions excludes those file extensions from testing.
Risk	If the file exclusions filter does not perform as expected, the system administrator will be notified of files that do not need to be included in the check. This extra information would flood the administrator with data and cause them to miss critical changes. The likelihood of this happening is dependent on the quality control of the vendor. The consequences could be high.
Risk Rating	Likelihood 2 Consequence 1 = Low Priority
Reference	CobiT
Test	Have the administrator: 1. Start the configuration interface by selecting start -> programs -> LANguard File Integrity Checker configuration. After the configuration interface (Ref Figure 1) starts, click excluded extensions then add, type “txt” then click ok then close to close the dialog box, then click ok to exit the configuration interface. 2. Use the import utility to import a list of file extensions by creating a text file with txt, doc, and tmp on a separate line for each extension; this can be done with notepad. Start the configuration interface then click excluded extensions then import, select the file that was just created, click open, after the dialog box is populated, click ok then close to close the dialog box, then click ok to exit the configuration. 3. Run a check on the system by selecting start -> programs -> LANguard File Integrity-> Checker check now. 3. Examine the output report for items that should be excluded.
Result	
Compliance	The results of this test are binary. Excluded items should not be reported.
Objective Subjective	Objective
Pass/Fail	

Test Item 24 Command Line Options

Control Objective	Validate application operation of command line starting and switches
Risk	According to the vendor documentation, the command to start the configuration interface from the command prompt or script is “cfcommand c”. If any other characters are accepted, the application may not perform as expected. There could be an unknown buffer overflow, or the application may not perform as expected.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Have the administrator start the command prompt and change directories to C:\Program Files\LANguard File Integrity Checker. Enter the command Cfservice with other any character(s) than “c” and observe the applications reaction.
Result	
Compliance	The results of this test are binary. The application should only accept the “c” option. All other characters should be disregarded by the application.
Objective Subjective	Objective
Pass/Fail	

Audit trail

Audit trails are essential when reconstructions of events are necessary.

Test Item 25 Application Logs

Control Objective	Techniques have been implemented for using and monitoring system utilities.
Risk	The application should keep logs of when the application was run and the results of the run. The lack of logs will make it harder to determine if the application is running as expected.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Examine the applications log file for time, date, and result of activity.
Result	
Compliance	The results of this test are binary. Time, date, and activity should be part of the logs.
Objective Subjective	Objective
Pass/Fail	

Test Item 26 Operating System Logs

Control Objective	Techniques have been implemented for using and monitoring system utilities.
Risk	The operating system should keep a log of when system security software is run, what userID was associated with the application. The lack of logs will make it harder to determine what userID is associated with the application, and if the application is running as expected.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Examine the operating system logs (security, application, and system) for evidence of application activity. Items such as time, date, and userID activity should be present. To view these logs, have the administrator log onto the computer. Navigate to Start->Programs->Administrative tools->Event Viewer. Once the event viewer starts, examine the three logs (security, application, and system) for evidence of LANguard File Integrity application activity.
Result	
Compliance	The results of this test are binary. Time, date, and activity should be part of the logs.
Objective Subjective	Objective
Pass/Fail	

Assignment 3 –Perform the Audit

To perform the audit, the checklists from assignment two will be utilized along with the flowchart located in appendix A. Application input controls are discussed in tests 8, 11, 12 and 22-24. Processing controls are discussed in tests 7, 13-21, and 25. Application output control is discussed in test 6. The method that will be utilized is one subdirectory and five test files will be created and added to the system to simulate different types of files by using simulated files, there is no risk to modifying real system files.

Risk Rating

Risk rating is a quantifiable measurement of the consequence if the control objective is not met. The risk rating allows management to prioritize deficiencies. High priority issues should be addressed first.

Risk Rating = Likelihood X Consequence

Likelihood	Consequence
1 = Unlikely	**1 = Minor impact**
2 = Possible	**2 = Major Impact**
3 = Probable	**3 = Critical Impact**

Risk Rating

1 or 2	=	Low priority
3 or 4	=	Medium priority action
6 or 9	=	High priority action

Policy/Procedure Review

Documentation review is the first step to determining what the rules are in the organization and who is assigned what responsibilities. Among the policies and procedures that require review are system software change controls and incident response. These policies/procedures should exist and be current.

Test Item 1 Documentation Review

Control Objective	Detailed Policy/Procedure review

Risk	Policies and procedures are the rules that all employees must follow. Not having computer security policies/procedures prohibits the company from having control over their resources and can leave the company vulnerable to unauthorized: computer usage, application installation, theft of company sensitive information, and confusion during an incident.
Risk Rating	Likelihood 3 Consequence 3 = High priority action
Reference	CobiT
Test	Review company computer security policies/procedures including, but not limited to, overall security policy, change management, and incident response for evidence of: • Confidentially, Integrity, Availability, Accountability statements Detailed change control and incident response procedures including: • On what basis changes should be approved • Who approves changes • Clearly stated roles and responsibilities • What the response is to unauthorized changes
Result	All policies and procedures are unwritten. All employees are told that they cannot load any software on the company's computers. Because the policies/procedures are un written, there is no evidence that can be provided.
Compliance	Compliance will be determined by how well documented the policies/procedures are.
Objective Subjective	Subjective
Pass/Fail	Fail

Test Item 2 Organizational review

Control Objective	Ensure proper segregation of duties
Risk	Improper segregation of duties can allow a single individual to take advantage of company resources for personal gain or to cover up inappropriate activities. These activities can range from misuse of resources to theft of company sensitive information/assets.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Review the companies organizational structure and job descriptions for proper segregation of duties.
Result	After interviewing the owner, he feels that the company is too small to have formal organizational documentation. There is no documentation on the structure of the company, therefore no evidence can be provided.
Compliance	Compliance will be determined by how well documented the policies/procedures are.

Objective Subjective	Subjective
Pass/Fail	Fail

Known Deficiency Research

Known deficiencies need to be identified in order to determine what the risks are to the version being audited.

Test Item 3 Application Patches

Control Objective	Determine if the product has any known deficiencies that adversely impact the application or security.
Risk	Product deficiencies could give an attacker the opportunity for exploit.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Visit the vendor website http://www.gfi.com/ and look for patches pertaining to LANguard File Integrity Checker. Go to the ICAT website (http://icat.nist.gov/icat.cfm) and look for vendor (GFI) and product (LANguard File Integrity Checker) vulnerabilities. If there are any patches or known weaknesses, ensure that the latest version is installed.
Result	No patches or known vulnerabilities found.
Compliance	The results of this test are binary. Either there are known weaknesses, or not. If there are known weakness the latest version should be installed. The version number is displayed on the configuration interface. To bring the application interface up, go to Start ->Programs->LANguard File Integrity Checker Configuration.
Objective Subjective	Objective
Pass/Fail	Pass

Identify All Access Paths

All access paths should be identified in order to determine what potential attackers could see.

Test Item 4 Network Path

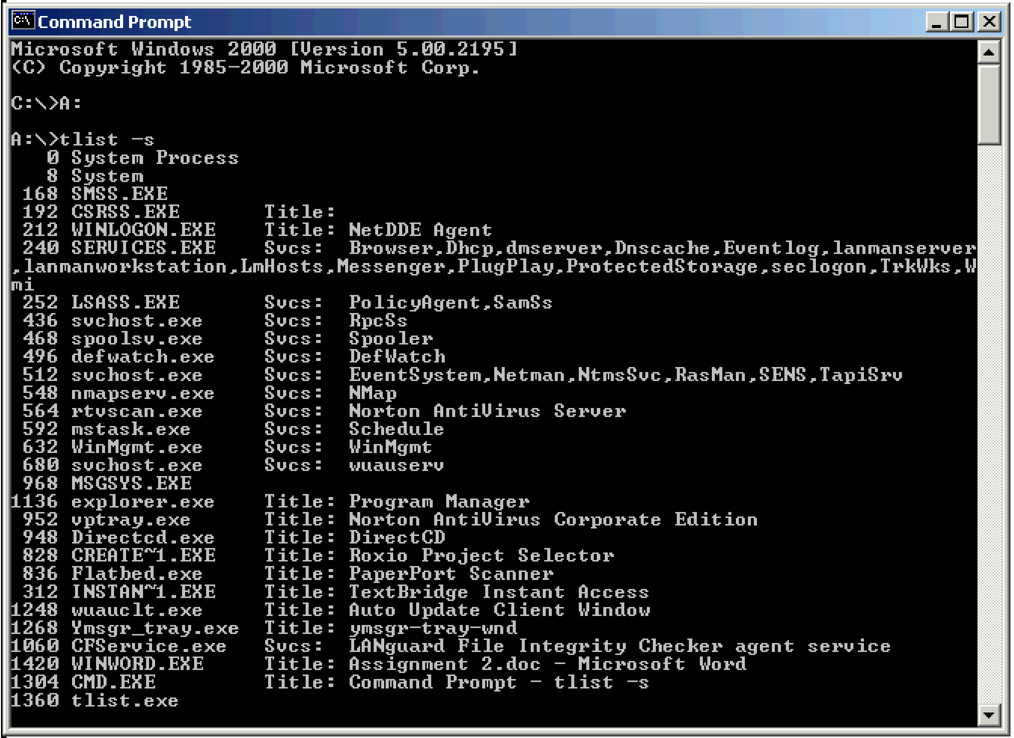
Control Objective	Evaluate controls over external access

Risk	Network visible services are an attackers first “look” at the system. If the file integrity service is visible, it could be vulnerable to a remote attack. If an attack is successful, the computer may become compromised, the attacker may be able to run code of his/her choice, or at least the application may not work as expected.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM, Vendor documentation Vendor documentation states that a service is installed (Cfservice) but does not indicate that it is network accessible.
Test	Utilizing a port scanner, scan all ports (65535 TCP/UDP) from another machine to determine if the service is visible from the network. The results should not reveal the “Cfservice” is running.
Result	nmap -sS -p 1-65535 -O -P0 192.168.1.100 Starting nmap V. 3.00 (www.insecure.org/nmap/) Interesting ports on (192.168.1.100): (The 65532 ports scanned but not shown below are in state: closed) Port State Service 135/tcp open loc-srv 139/tcp open netbios-ssn Remote operating system guess: Windows 2000/XP/ME Nmap run completed -- 1 IP address (1 host up) scanned in 18 seconds
Compliance	The results of this test are binary. The Cfservice should not be visible from the network.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 5 Host Path

Control Objective	Identify all access paths
Risk	There should not be any services running under the application service (Cfservice). If there is then the other service should be investigated for possible malicious activity. The vendor information does not indicate that any other service is running under the Cfservice.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM

<table>
<tr><td>Test</td><td>Using the application Tlist.exe from the Microsoft Windows 2000 Installation CD (This application must be extracted prior to use. Navigate to Support\Tools folder on the Windows 2000 installation CD; extract the Tlist.exe utility from the Support.cab file). From the command prompt, change directories to the location that tlist.exe was extracted to and type the command Tlist –s. The output from Tlist.exe will show what services are running under each process. The –s option shows services active for each process in a tree view. For more information see http://is-it-true.org/nt/atips/atips301.shtml</td></tr>
<tr><td>Result</td><td>Tlist -s output



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>A:

A:\>tlist -s
   0 System Process
   8 System
 168 SMSS.EXE
 192 CSRSS.EXE       Title:
 212 WINLOGON.EXE    Title: NetDDE Agent
 240 SERVICES.EXE    Svcs:  Browser,Dhcp,dmserver,Dnscache,Eventlog,lanmanserver
,lanmanworkstation,LmHosts,Messenger,PlugPlay,ProtectedStorage,seclogon,TrkWks,W
mi
 252 LSASS.EXE       Svcs:  PolicyAgent,SamSs
 436 svchost.exe     Svcs:  RpcSs
 468 spoolsv.exe     Svcs:  Spooler
 496 defwatch.exe    Svcs:  DefWatch
 512 svchost.exe     Svcs:  EventSystem,Netman,NtmsSvc,RasMan,SENS,TapiSrv
 548 nmapserv.exe    Svcs:  NMap
 564 rtvscan.exe     Svcs:  Norton AntiVirus Server
 592 mstask.exe      Svcs:  Schedule
 632 WinMgmt.exe     Svcs:  WinMgmt
 680 svchost.exe     Svcs:  wuauserv
 968 MSGSYS.EXE
1136 explorer.exe    Title: Program Manager
 952 vptray.exe      Title: Norton AntiVirus Corporate Edition
 948 Directcd.exe    Title: DirectCD
 828 CREATE~1.EXE    Title: Roxio Project Selector
 836 Flatbed.exe     Title: PaperPort Scanner
 312 INSTAN~1.EXE    Title: TextBridge Instant Access
1248 wuauclt.exe     Title: Auto Update Client Window
1268 Ymsgr_tray.exe  Title: ymsgr-tray-wnd
1060 CFService.exe   Svcs:  LANguard File Integrity Checker agent service
1420 WINWORD.EXE     Title: Assignment 2.doc - Microsoft Word
1304 CMD.EXE         Title: Command Prompt - tlist -s
1360 tlist.exe
```

By examining process ID 240, you will see multiple services running under the services.exe process. Process ID 1060 is the Cfservice running, there are no other services running under this process.</td></tr>
<tr><td>Compliance</td><td>The results of this test are binary. No other services should be running under the Cfservice process.</td></tr>
<tr><td>Objective
Subjective</td><td>Objective</td></tr>
<tr><td>Pass/Fail</td><td>Pass</td></tr>
</table>

Data Integrity

Data that is sent from one computer to another is subject to interception and manipulation. Data integrity ensures that the information that is received is exactly the information that was sent without manipulation.

Test Item 6 Report Protection

Control Objective	Protection of sensitive messages in-transit.
Risk	If the report is intercepted and manipulated in-transit and there is no mechanism to detect this type of activity, the system administrator may not receive an accurate report. This could significantly impact the decision process.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Examine the report for evidence of a digital signature.
Result	No evidence of a digital signature <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:37:13 ** ***************** - C:\TestFolder\ has changed! Folder: TestFolder Creation Date: 09/15/02 11:21:42 Modification Date: 09/15/02 11:37:07 - C:\TestFolder\testFile5.doc removed from the system! File: testFile5.doc Size: 0 ** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The report should be digitally signed to detect in-transit manipulation.
Objective Subjective	Objective
Pass/Fail	Fail

Test Item 7 Cryptographic Signature

Control Objective	Verify that a cryptographic file integrity signature is created

Risk	If the file integrity signature is not encrypted, i.e. MD5, SHA1 etc. an attacker could alter the signature to hide their activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	CobiT
Test	Have the administrator 3. Open the Cfdata.mdb database 4. Open the "old_Data" table and verify that a hash value for the files has been created.
Result	**PATH** **FILENAME** **MD5** **SIZE** TestFolder testFile4.txt 46b1a48689b8e96c78041e5ab4b057ea 137
Compliance	The results of this test are binary. There should be a hash value for each file in the database
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 8 Full File Name

Control Objective	Verify that the full filename is reported
Risk	It is imperative that the application reports the full file name. If the full file name is not reported, it may be very difficult to determine exactly which file was altered.
Risk Rating	Likelihood 3 Consequence 2 = High priority action
Reference	CobiT
Test	Windows 2000 has a maximum of 215 characters for a file name. Create a test file with 215 characters. Run the application and verify that the full file name has been reported.

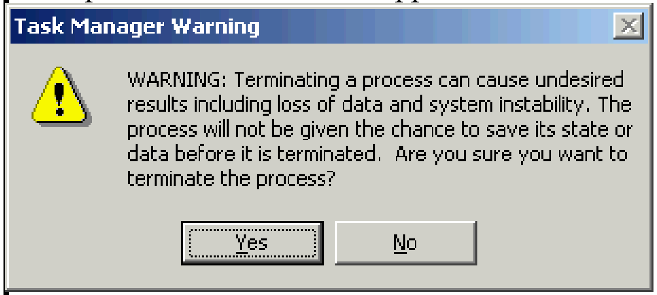
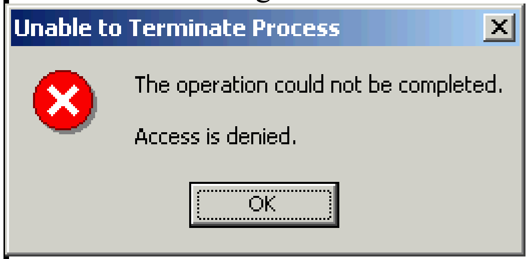
Result	The application did detect and report the full 215 character file name <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:25:06 *** ***************** - C:\TestFolder\ has changed! Folder: TestFolder Creation Date: 09/15/02 11:21:42 Modification Date: 09/15/02 11:24:43 - C:\TestFolder\Aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.txt was added to the system! File: Aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.txt Size: 0 Creation Date: 09/15/02 11:24:43 Modification Date: 09/15/02 11:24:43 *** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The application should detect and report the full file name.
Objective Subjective	Objective
Pass/Fail	Pass

Least Privilege

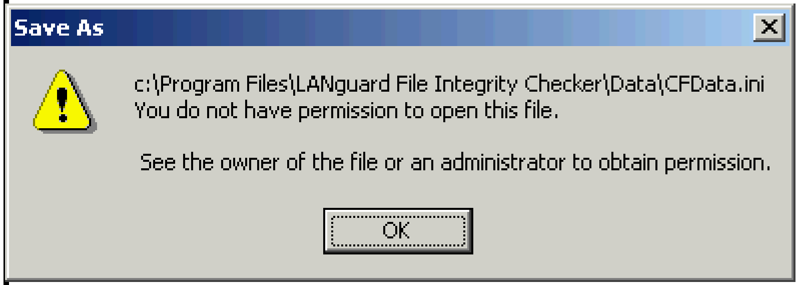
Least privilege is the control that ensures only persons that require access to sensitive applications/utilities have that access. Access by all other persons should be denied.

Test Item 9 Service Security

Control Objective	Ensure least privilege.

Risk	If non-administrators have access to the application or its underlying service, proper operation of the application cannot be ensured. It would be possible for internal users to hide their activities.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Log on with user permissions and attempt to stop the application by 1. Start the task manager by pressing ctrl + alt + del. 7. Select Task manager 8. Select the Processes tab 9. Select Cfservice.exe 10. Click End Process 11. Acknowledge the task manager warning by clicking yes
Result	The user was unable to stop the service. Attempt to end the Cfservice application  Task Manager Warning WARNING: Terminating a process can cause undesired results including loss of data and system instability. The process will not be given the chance to save its state or data before it is terminated. Are you sure you want to terminate the process? Results after clicking Yes  Unable to Terminate Process The operation could not be completed. Access is denied.
Compliance	The results of this test are binary. After clicking yes at the task manager warning, There should be a message that states, “Unable to terminate process access is denied”.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 10 Protect Configuration Files

Control Objective	Configuration file protection
Risk	Without proper change control, the configuration files could be modified preventing the application from functioning or processing irregularities could be introduced.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Log on to the computer with user permissions and attempt to modify the initialization configuration file located at C:\Program Files\LANguard File Integrity Checker\Data\CFData.ini by adding three (3) characters to the end of the file.
Result	The applications configuration files could not be modified.  Save As c:\Program Files\LANguard File Integrity Checker\Data\CFData.ini You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.
Compliance	The results of this test are binary. Anyone without explicit authorization should not be able to modify the configuration or associated files.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 11 Application Schedule

Control Objective	Determine scheduler controls and access authorizations.
Risk	If the users can access the schedule, they could modify it or disable the schedule completely. If the users did disable the schedule, the application would not run resulting in a high risk of unauthorized file modification.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM

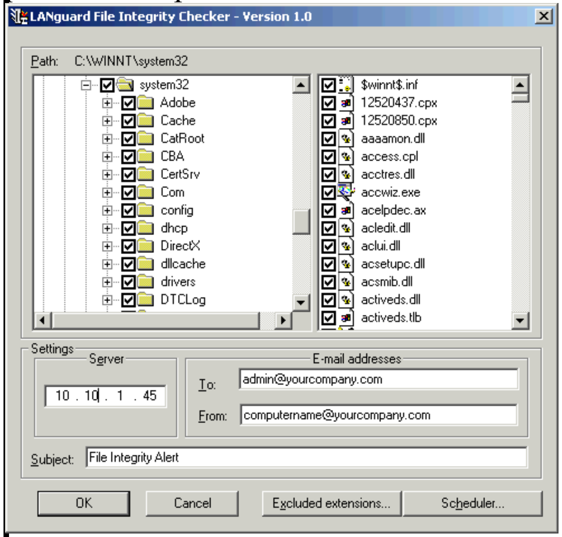
Test	Have the administrator use the built-in scheduler and schedule a file check with the administrator user ID and password. Have the administrator log out and have a non-privileged user log in. The scheduled task should complete. With the non-privileged user logged in, examine the task scheduler for the LANguard File Integrity Checker schedule. The scheduled job should not be visible.
Result	Both tests passed. The schedule executed as expected, The task was not visible to the user.
Compliance	The results of this test are binary. The scheduled task should not be visible to the non-privileged user and the application should run as expected.
Objective Subjective	Objective
Pass/Fail	Pass

Inappropriate/Unusual Activities Detected

This is what file integrity verification software is designed to do. If the application does not detect inappropriate/unusual activities, then the application fails to provide a useful function.

Test Item 12 Files Identified

Control Objective	All critical files are identified.
Risk	This type of application verifies the integrity of files. If critical files are not identified and monitored, the application will not provide information on the status of critical files
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Navigate to start->program files-> LANguard File Integrity Checker -> LANguard file integrity checker configuration. Review all files that have been selected. These should be files that are not expected to change.

Result	The files that are selected are not expected to change. There is no mechanism to print the complete list.  LANguard File Integrity Checker - Version 1.0 Path: C:\WINNT\system32 ☑ system32 ☑ Adobe ☑ Cache ☑ CatRoot ☑ CBA ☑ CertSrv ☑ Com ☑ config ☑ dhcp ☑ DirectX ☑ dllcache ☑ drivers ☑ DTCLog ☑ $winnt$.inf ☑ 12520437.cpx ☑ 12520850.cpx ☑ aaaamon.dll ☑ access.cpl ☑ acctres.dll ☑ accwiz.exe ☑ acelpdec.ax ☑ acledit.dll ☑ aclui.dll ☑ acsetupc.dll ☑ acsmib.dll ☑ activeds.dll ☑ activeds.tlb Settings Server: 10 . 10 . 1 . 45 E-mail addresses To: admin@yourcompany.com From: computername@yourcompany.com Subject: File Integrity Alert
Compliance	This is a subjective test but, selected files should include executables (.exe), dynamic link libraries (.dll), system files (.sys), device drivers (.vxd) etc…
Objective Subjective	Subjective
Pass/Fail	Pass

Test Item 13 Addition of New Users

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report the addition of new users to the system
Risk	When adding a new user to the system, the SAM file will change and there should be an audit trail to determine if it was an authorized user or an attacker.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Have the system administrator add a new user to the system and run the application select start ->programs -> LANguard File Integrity Checker -> check now. Examine the output of the application for a modified SAM file.

Result	The report shows that the SAM file was changed but there is no indication of file size change. <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/13/02 00:11:15 ** ****************** - C:\WINNT\system32\config\SAM has changed! File: SAM Size before change: 24576 Size after change: 24576 Size difference: 0 - C:\WINNT\system32\config\default has changed! File: default Size before change: 163840 Size after change: 163840 Size difference: 0 ** ****************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The SAM file should show that it was modified.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 14 Files Added

Control Objective	Inappropriate or unusual activities detected for files added.
Risk	This test is necessary to determine if an attacker has compromised the computer or if rouge software is added to the system.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Add a test file to the system and run the application. Examine the output report for the addition of the test file.

Result	The application did detect and report files that were added. <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:23:17 ** **************** - C:\TestFolder\testFile1.exe was added to the system! File: testFile1.exe Size: 0 Creation Date: 09/15/02 11:23:05 Modification Date: 09/15/02 11:23:05 ** **************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The report should show that a file was added to the system.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 15 Files Deleted

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report files deleted
Risk	Files that have been deleted could be an indication that the system needs to be examined for attacker activity or malicious code.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Delete the test file that was added in the previous step and run the application. Examine the output for the deletion of the test file.

Result	The deleted file was detected and reported <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:37:13 ** ***************** - C:\TestFolder\ has changed! Folder: TestFolder Creation Date: 09/15/02 11:21:42 Modification Date: 09/15/02 11:37:07 - C:\TestFolder\testFile1.exe removed from the system! File: testFile1.exe Size: 0 ** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The report should show that the file was removed from the system.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 16 Files Modified

Control Objective	Inappropriate or unusual activities detected for file content modification.
Risk	Unauthorized file content modification could be an indication of attacker activity.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Modify the content of a test file by adding three (3) characters and run the application. Examine the output for evidence of the test file modification.

Result	Modified files are detected and reported. <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:39:11 *** ***************** - C:\TestFolder\testFile4.txt has changed! File: testFile4.txt Size before change: 0 Size after change: 3 Size difference: 3 *** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The report should indicate that the file was modified.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 17 File Attribute Change

Control Objective	Inappropriate or unusual activities detected. The application should detect and report file attribute changes (i.e.. Hidden, System, Read Only)
Risk	Attackers try to hide their tools. The application should detect these changes.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Utilizing the tool Properties Plus, change the attributes of three (3) test files to hidden, system, read only, and run the application. Examine the output for the attribute changes of the test files.
Result	The application failed to detect or report file attribute changes. Without a report, there is no evidence available.
Compliance	The results of this test are binary. File attribute changes should be detected and reported.
Objective Subjective	Objective
Pass/Fail	Fail

Test Item 18 File Date and Time Changes

Control Objective	Inappropriate or unusual activities detected. Does the application detect and report file time and date changes
Risk	Attackers can alter file dates and times to conceal their activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Utilizing the tool Properties Plus (available from http://www.ne.jp/asahi/cool/kish/), Change the date on one of the test files and the time on another test file and run the application. Examine the output for the modification of dates and times of the test files.
Result	The application failed to detect and report file time and date changes. Without a report, there is no evidence available.
Compliance	The results of this test are binary. The application should detect and report the time and date change if the test files.
Objective Subjective	Objective
Pass/Fail	Fail

Test Item 19 Time and Date of File Change

Control Objective	Inappropriate or unusual activities detected. Does the application report the time and date of file changes.
Risk	Reporting the time and date of change is critical in determining when the activity took place. It is a step in reconstructing the attackers activities.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Modify one of the test files and run the application. Examine the output of the report for date and time of file change.

Result	The application fails to report the time and date for changes to files. There is no evidence of when the file was changed <E-mail header removed> Date: Sunday, September 15, 2002 12:00 PM This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:57:11 ** ***************** - C:\TestFolder\testFile2.dll has changed! File: testFile2.dll Size before change: 0 Size after change: 0 Size difference: 0 ** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The report should indicate the time and date of the file change.
Objective Subjective	Objective
Pass/Fail	Fail

Test Item 20 File Size Difference

Control Objective	Inappropriate or unusual activities detected. Does the application report before, after, and difference of file size.
Risk	This is necessary to determine if data was added or deleted. Configuration file alterations could lead to the masking of attacker activities.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Modify two (2) test files. One to increase the size of the file by adding three characters. Modify the other test file to remove three characters. Run the application. Examine the output report for file size before, after, and difference on the test files that have been modified.

Result	The application did report the before, after, and size difference of a modified file. <E-mail header removed> This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:39:11 ** ***************** - C:\TestFolder\testFile4.txt has changed! File: testFile4.txt Size before change: 0 Size after change: 3 Size difference: 3 ** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. Before and after file size should be reported.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 21 New Subdirectory

Control Objective	Inappropriate or unusual activities detected. Determine if the application will detect a newly created subdirectory.
Risk	Attackers typically add subdirectories to place their files.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	FISCAM
Test	Create a subdirectory by navigating to start ->programs->accessories-> windows explorer. Select the C drive and go to the menu, file->new folder. Run the application and examine the report to determine if the application detected the new subdirectory.

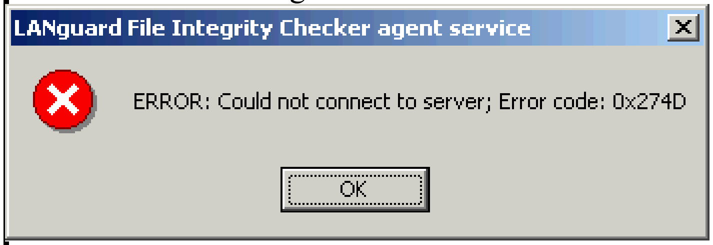
Result	The application did detect and report the addition of a new subdirectory. This is an automatic message. Do not reply ! Report generated by LANguard File Integrity Checker on 09/15/02 11:23:17 ** ***************** - C:\TestFolder\ was added to the system! Folder: TestFolder Creation Date: 09/15/02 11:21:42 Modification Date: 09/15/02 11:23:05 ** ***************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. The application should detect and report that a new folder was added to the system.
Objective Subjective	Objective
Pass/Fail	Pass

Validate Application

These tests are specific to the application.

Test Item 22 Non-SMTP Server Address

Control Objective	Validate application operation
Risk	Misconfiguration would prevent the application from sending the report. If the report cannot be sent, the system administrator will not be notified of changes.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Enter an IP address that is not a SMTP server. This test will validate error messages indicating a misconfiguration. Ref Figure 1

Result	On screen error message  ERROR: Could not connect to server; Error code: 0x274D Error message on screen and in the logs. September 15, 2002 12:03:41 937 Start September 15, 2002 12:04:44 497 ERROR: Could not connect to server; Error code: 0x274D September 15, 2002 12:04:44 687 Stop
Compliance	The results of this test are binary. There should be an error message indicating that the application cannot send the report.
Objective Subjective	Objective
Pass/Fail	Pass

Test Item 23 File Exclusions

Control Objective	Validate application operation to determine if the list of excluded file extensions excludes those file extensions from testing.
Risk	If the file exclusions filter does not perform as expected, the system administrator will be notified of files that do not need to be included in the check. This extra information would flood the administrator with data and cause them to miss critical changes. The likelihood of this happening is dependent on the quality control of the vendor. The consequences could be high.
Risk Rating	Likelihood 2 Consequence 1 = Low priority action
Reference	CobiT

Test	Have the administrator: 1. Start the configuration interface by selecting start -> programs -> LANguard File Integrity Checker configuration. After the configuration interface (Ref Figure 1) starts, click excluded extensions then add, type "txt" then click ok then close to close the dialog box, then click ok to exit the configuration interface. 2. Use the import utility to import a list of file extensions by creating a text file with txt, doc, and tmp on a separate line for each extension; this can be done with notepad. Start the configuration interface then click excluded extensions then import, select the file that was just created, click open, after the dialog box is populated, click ok then close to close the dialog box, then click ok to exit the configuration. 3. Run a check on the system by selecting start -> programs -> LANguard File Integrity-> Checker check now. 3. Examine the output report for items that should be excluded.
Result	Excluded items are still checked and reported. This is an automatic message. Do not reply ! <E-mail header removed> Report generated by LANguard File Integrity Checker on 09/15/02 12:01:46 *** ****************** - C:\TestFolder\testFile4.txt has changed! File: testFile4.txt Size before change: 15 Size after change: 24 Size difference: 9 *** ****************** For the latest version and more free software visit: http://www.gfi.com
Compliance	The results of this test are binary. Excluded items should not be reported.
Objective Subjective	Objective
Pass/Fail	Fail

Test Item 24 Command Line Options

Control Objective	Validate application operation of command line starting and switches

Risk	According to the vendor documentation, the command to start the configuration interface from the command prompt or script is "cfcommand c". If any other characters are accepted, the application may not perform as expected. There could be an unknown buffer overflow, or the application may not perform as expected.
Risk Rating	Likelihood 2 Consequence 3 = High priority action
Reference	CobiT
Test	Have the administrator start the command prompt and change directories to C:\Program Files\LANguard File Integrity Checker. Enter the command Cfservice with other any character(s) than "c" and observe the applications reaction.
Result	The application silently disregards other switches
Compliance	The results of this test are binary. The application should only accept the "c" option. All other characters should be disregarded by the application.
Objective Subjective	Objective
Pass/Fail	Pass

Audit trail

Audit trails are essential when reconstructions of events are necessary.

Test Item 25 Application Logs

Control Objective	Techniques have been implemented for using and monitoring system utilities.
Risk	The application should keep logs of when the application was run, the results of the run, and provide individual accountability. The lack of logs will make it harder to determine the status of integrity checks and what account (userID) the application was run under.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Examine the applications log file for time, date, and result of activity.

Result	The application does log activity. September 15, 2002 11:56:05 921 Start September 15, 2002 11:56:08 115 Stop September 15, 2002 11:57:09 893 Start September 15, 2002 11:57:12 187 Stop September 15, 2002 11:57:29 421 Start September 15, 2002 11:57:30 944 Stop September 15, 2002 11:58:57 969 Start September 15, 2002 11:58:59 491 Stop September 15, 2002 11:59:55 331 Start September 15, 2002 11:59:56 853 Stop September 15, 2002 12:01:21 85 Start September 15, 2002 12:01:25 220 Stop September 15, 2002 12:01:45 299 Start September 15, 2002 12:01:47 322 Stop
Compliance	The results of this test are binary. Time, date, activity, and userID should be part of the logs.
Objective Subjective	Objective
Pass/Fail	Pass with exception of what userID the application was running under

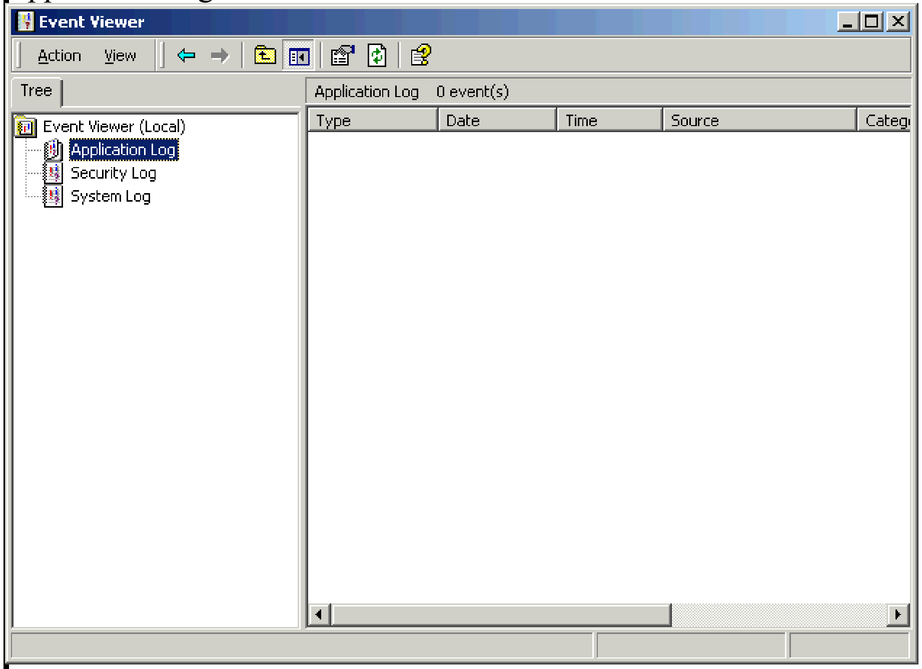
Test Item 26 Operating System Logs

Control Objective	Techniques have been implemented for using and monitoring system utilities.
Risk	The operating system should keep a log of when system security software is run, what userID was associated with the application. The lack of logs will make it harder to determine what userID is associated with the application, and if the application is running as expected.
Risk Rating	Likelihood 2 Consequence 2 = Medium priority action
Reference	FISCAM
Test	Examine the operating system logs (security, application, and system) for evidence of application activity. Items such as time, date, and userID activity should be present. To view these logs, have the administrator log onto the computer. Navigate to Start->Programs->Administrative tools->Event Viewer. Once the event viewer starts, examine the three logs (security, application, and system) for evidence of LANguard File Integrity application activity.

<table>
<tr>
<td>Result</td>
<td>

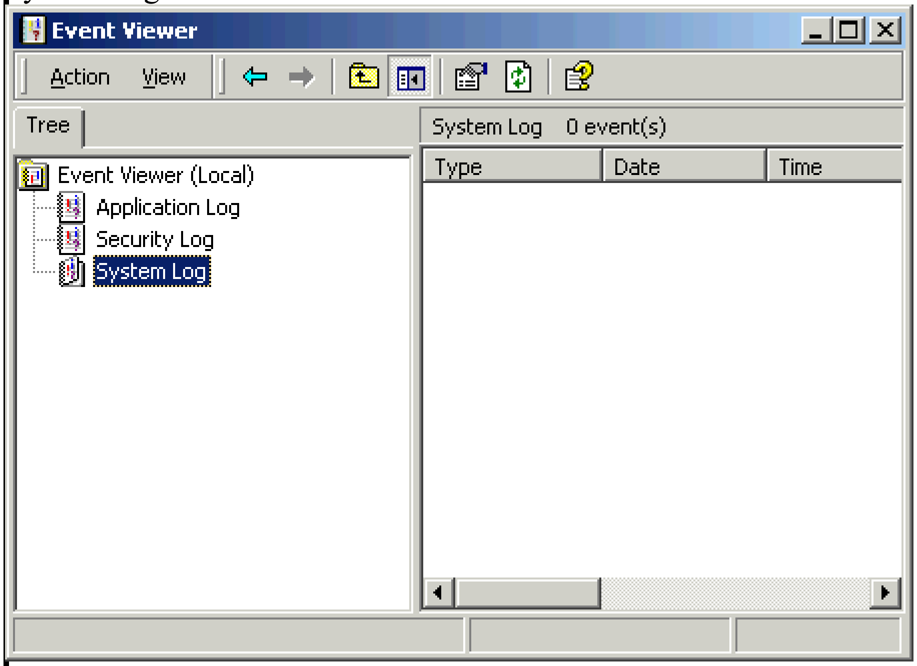
There is no evidence that the operating system is configured to log application events.

Application Logs



Application Log 0 event(s)

System Logs



System Log 0 event(s)

</td>
</tr>
</table>

Compliance	The results of this test are binary. Time, date, and activity should be part of the logs.
Objective Subjective	Objective
Pass/Fail	Fail

Is the application securable?

The primary goal of this audit is to ensure that company policies regarding system software change control are being followed. The secondary goal is to validate vendor claims and to ensure that the file integrity application maintains availability, integrity, confidentially. After performing the audit, it is my opinion that this audit process was a success.

LANguard File Integrity Checker does fulfill the requirements for this audit even though not all of the control objectives passed testing. I discovered that without clear and concise policies/procedures, there is no clear direction or accountability for employees. The application does not maintain the confidentiality or integrity of messages in-transit, it does not detect or report file date, time, or attribute changes. The report that the system administrator receives does not contain the date and time that files were changed. The file exclusion feature does not prevent the detection or reporting of excluded file extensions.

Is the application auditable?

At the time of this writing, there were no existing audit checklists or guidelines. In the absence of existing checklists and guidelines, a checklist was developed using control objectives from CobiT and FISCAM. One area that was not covered is secure off line storage of the database. This should be part of the organizations security policy. All of the manufacturers claims were verifiable and verified. Any specific requirements other than the ones in this paper would come from an organizations computer policy.

Assignment 4 – Follow Up

Executive Summary

The primary goal of this audit was to ensure that company policies/procedures regarding system software change control are being followed. The role of LANguard File Integrity Checker is to notify the system administrator of added, deleted, or modified files within the organization's computer systems. The application should perform as advertised (detect and report file additions, deletions, and modifications), be securable against unauthorized configuration modifications, capable of secure scheduled operations, and be protected from user attempts to stop the application.

Overall, the objectives of this audit were met. The application does detect the addition, deletion, and modification of files. The application is also schedulable and securable from the unprivileged users. However, there are no policies/procedures in place to control the change control process.

Eight specific findings resulted from this audit. These findings are ranked from high risk to low risk.

- No documented policies/procedures
  - The lack of policies/procedures prohibits the company from having control over their resources and can leave the company vulnerable to unauthorized: computer usage, application installation, and theft of company sensitive information, and confusion with roles and responsibilities.
- No company organization documentation to ensure proper segregation of duties
  - Improper segregation of duties can allow a single individual to take advantage of company resources for personal gain or to cover up inappropriate activities.
- The report that the system administrator receives from the application does not contain a digital signature or a hash value
  - By not having a digital signature or hash value, the e-mailed report can be intercepted and modified. This can lead to an inaccurate report that hides attacker activities.
- File attribute changes (hidden and read-only) are not detected or reported by the application
  - Attackers try to hide their tools by changing the attributes of their files.

- File date and time changes are not detected or reported
  - The file date and time change reporting is critical in determining when the activity took place. It is a step in reconstructing the attackers activities.

The consequence would be a loss of the audit trail and extended time necessary for an investigation.

- The date and time that files were modified is not reported
    - Attackers can alter file dates and times to conceal their activities. It will appear that there was no activity on the system during a questionable time-period.
- The file exclusions feature does not perform as expected. There are two different ways to exclude files from being checked, the GUI and an import utility.
    - The system administrator will be notified of files that do not need to be included in the check. This extra information would flood the administrator with data and cause them to miss critical changes.

- Application logs do not provide evidence of individually accountability.
    - A lack of individual accountability exists

Audit Findings

Overall, the audit of GFI's LANguard File Integrity Checker (v 1.0) produced very few findings. Below are the deficiencies that the audit has uncovered. They are ranked high risk to low risk.

Audit finding 1 *(Ref. Test Item 1. 2)* ***Risk rating High*** No policies/procedures or organizational documentation.

Risks: The lack of policies/procedures prohibits the company from having control over their resources and can leave the company vulnerable to unauthorized: computer usage, application installation, theft of company sensitive information, and/or confusion with roles and responsibilities.

Recommendation: Proper segregation of duties and job responsibilities should be clearly documented and enforced. Policies and procedures should be written, not only for the change control process, but also for all other processes. Policies and procedures are the rules that all employees must follow. They are the building blocks on which all activities are based.

Cost: Policies can be purchased and modified, or they can be written from scratch. Pre written policies can range from 500 to 1500 dollars and are easily tailored to meet company requirements. Creating policies from scratch could potentially be more expensive because of the level of knowledge and experience necessary to write good policies.

Compensating controls: There are no compensating controls for this risk.

Audit finding 2 *(Ref. Test Item 6)* ***Risk rating High*** The report that the system administrator receives from the application does not contain a digital signature or a hash value.

Risks: By not having a digital signature or hash value, the e-mailed report can be intercepted and modified. This can lead to an inaccurate report that hides attacker activities.

Recommendation: Option 1. Establish a secure communication path between the host and the server; Option 2. Request the vendor to add this functionality.

Cost: For option 1 the time required would be less than one hour per machine. For option 2, there is no cost incurred.

Compensating controls: There are no compensating controls for this risk.

Audit Finding 3 (Ref. Test Item 17) ***Risk rating High*** File attribute changes (hidden and read-only) are not detected or reported by the application.

Risks: Attackers try to hide their tools by changing the attributes of their files.

Recommendation: Ensure that the option is set to display hidden files and folders.

Cost: There are no costs to this recommendation.

Compensating controls: As the last line of defense, the only other compensating controls are the methods used to set permission on the computer.

Audit finding 4 (Ref. Test Item 18) ***Risk rating Medium*** File date and time of changes are not detected or reported.

Risks: Reporting the time and date of change is critical in determining when the activity took place. It is a step in reconstructing the attackers activities. The consequence would be a loss of the audit trail and extended time necessary for an investigation.

Recommendation: Request the vendor to add this functionality.

Cost: There are no costs to this recommendation

Compensating controls: As the last line of defense, the only other compensating controls are the methods used to set permission on the computer.

Audit finding 5 (Ref. Test Item 19) ***Risk rating Medium*** The date and time that files were modified is not reported.

Risks: Attackers can alter file dates and times to conceal their activities. It will appear that there was no activity on the system during a questionable time-period.

Recommendation: Request the vendor to add this functionality.

Cost: There are no costs to this recommendation

Compensating controls: As the last line of defense, the only other compensating controls are the methods used to set permission on the computer.

Audit Finding 6 (Ref. Test Item 23) ***Risk rating Low*** The file exclusions feature does not perform as expected. There are two different ways to exclude files from being checked, the GUI and an import utility.

Risks: If the file exclusions filter does not perform as expected, the system administrator will be notified of files that do not need to be included in the check. This extra information would flood the administrator with data and may allow critical changes to be missed.

Recommendation: Manually set the files and folders to be checked.

Cost: The only cost to this is time. It would take approximately two hours to develop the initial baseline and approximately one-half hour to set each of the other computers.

Compensating controls: There are no compensating controls for this.

Audit finding 7 (Ref. Test Item 25) ***Risk rating Low*** Application logs do not provide evidence of individual accountability.

Risks: The lack of logs will make it harder to determine the status of integrity checks and what account (userID) the application was run under.

Recommendation: Enable application logging at the operating system level. This will log the application activity and provide individual accountability.

Cost: None

Compensating controls: Operating system logs can compensate for this item.

References

COBIT Steering Committee and IT Governance Institute "Control Objectives for Information and Related Technology", Third Edition, July 2000.

United States General Accounting Office "Federal Information System Controls Audit Manual" (FISCAM), GAO/AIMD-12.19.6, January 1999

GFI LANguard File integrity checker Version 1.0 URL http://www.gfi.com/languard/lantools-fic.htm

Hoelzer, David "Auditing principles and concepts" SANS2002 Orlando, Fl April 2002

Kolde, Jennifer "Advanced systems audit" SANS2002 Orlando, Fl April 2002

Rauch, Jeremy. "Basic File Integrity Checking" August 14, 2000
URL http://online.securityfocus.com/infocus/1408

Tools

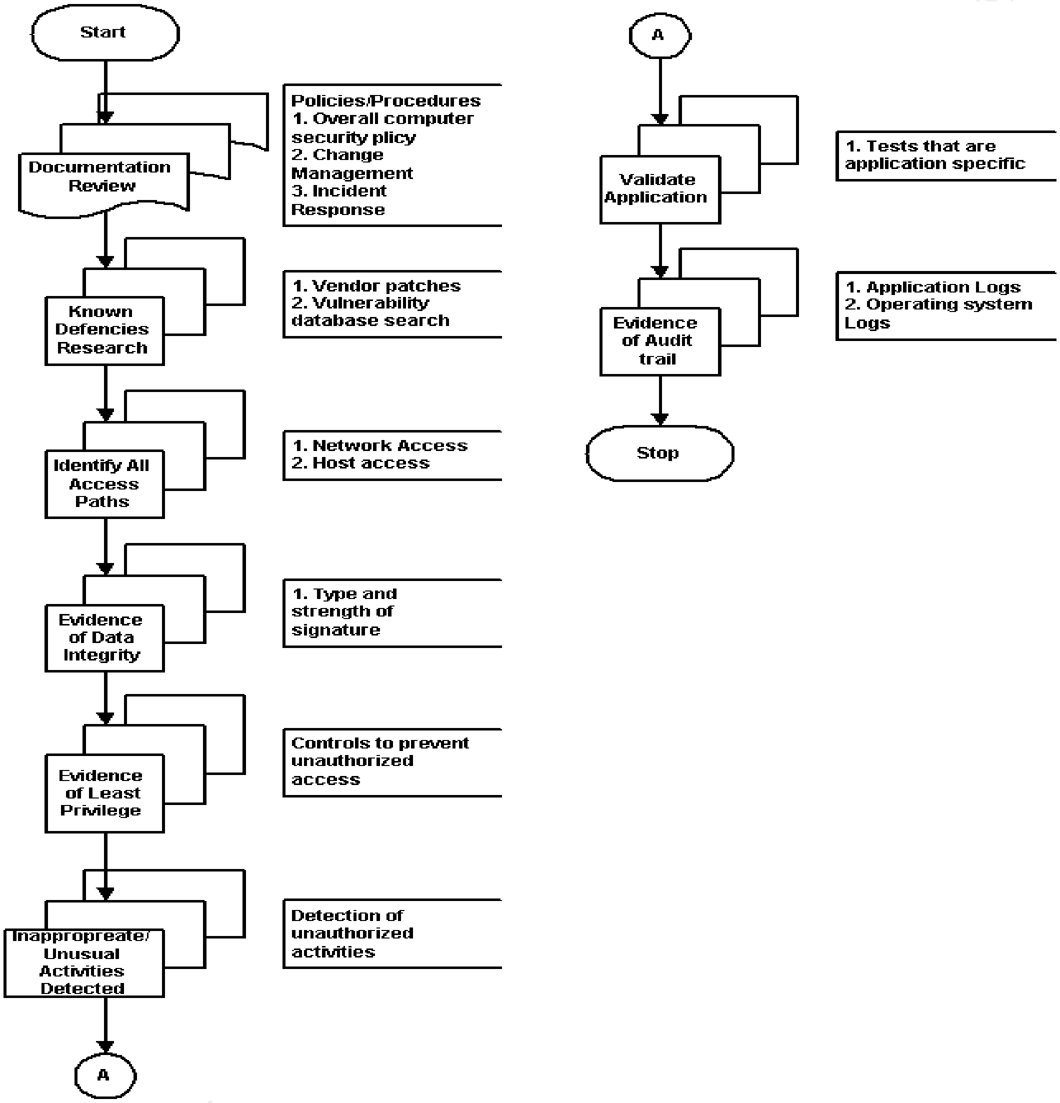
Nmap http://www.insecure.org/nmap

Tlist.exe Microsoft 2000 Professional Installation CD

Appendix A

Audit process flowchart

Step 1 is multi-document review. The remaining steps are multi-test steps.


Start
Documentation Review
Policies/Procedures
1. Overall computer security plicy
2. Change Management
3. Incident Response
Known Defencies Research
1. Vendor patches
2. Vulnerability database search
Identify All Access Paths
1. Network Access
2. Host access
Evidence of Data Integrity
1. Type and strength of signature
Evidence of Least Privilege
Controls to prevent unauthorized access
Inappropreate/ Unusual Activities Detected
Detection of unauthorized activities
A
A
Validate Application
1. Tests that are application specific
Evidence of Audit trail
1. Application Logs
2. Operating system Logs
Stop