Assessment and Evaluation of a General Purpose Portable Workstation Apple PowerBook OS X Configuration and Operational Practices

An Administrator's Perspective

Claude V. Lucas
CISSP, IAM

GSNA Practical V3.0 April 15, 2004

Table of Contents

Introduction

The primary purpose of this exercise is to demonstrate the author's knowledge of the methodologies, techniques, and tools used to examine an organization's information security posture, information security policies, and actual information security practices. This will be accomplished by performing a formal information security assessment and evaluation of the organization's information systems usage to measure compliance with both the organization's policies and with industry standard best accepted practices. A secondary purpose is to help the author coalesce the knowledge that he has gained from various sources such as the U.S Government's National Security Agency's unclassified "INFOSEC Assessment Methodology"[1] course as presented by Security Horizon, Inc., SANS "Auditing Networks, Perimeters and Systems" boot camp, and from several years direct experience in the information security field. This will be accomplished by assessing the author's own personal information security posture and evaluating his information security practices in regard to his personal laptop system. It is the author's sincere hope that this exercise will also be of benefit to others who may be contemplating the use of the IAM.

System Description

The target Apple PowerBook is used for a number of different and sometimes divergent purposes. It is used for most of the client's daily telecommunication needs including sending and receiving email and World Wide Web use. It is used to organize and archive various photographs and video clips. It is used to record, organize and archive both original and legally downloaded music files. It is used as a research and educational tool, and as a network, peripheral, application, and system technical evaluation platform. The operating system in use is the Apple Computer OS X, with no use of earlier Macintosh operating systems. In addition to OS X native applications, a limited usage of Microsoft Windows 2000 and Windows legacy applications is supported via another Microsoft product, "Virtual PC".

Scope of Assessment

A detailed assessment and evaluation of the security and efficacy of the application software or of the open source UNIX programs in use is outside the scope of this analysis, although some mention of software used by the target organization is included. Software in use, if updated to latest released version, will be presumed to be secure for the purpose of this exercise. Analysis of the Microsoft Windows 2000 installation and of various Windows applications running under MS Virtual PC is also outside of the scope of this investigation. Obviously, it is a severe case of "overkill" to apply the IAM to a single laptop system, but the methodology is both solid and scalable. The skills, tools, and techniques used in this exercise are applicable to the assessment and evaluation of far larger information systems than the current target.

[1] United States Government National Security Agency
Infosec Assessment Training and Rating Program
“IAM Home Page”
URL: http://www.iatrp.com/iam.cfm

Assessment, Evaluation, or Audit?[2]

These terms are often used interchangeably, but have distinctly different meanings to different audiences. For the purpose of this exercise, the author will define the terms as follows.

Assessment

An assessment is the analysis of the controls implemented to protect information that is transmitted, processed or stored by a system. It also is a measurement of the security posture of an organization. In most cases, an assessment involves no hands on testing or technical validation; rather it relies on demonstrations and interviews to validate control implementations. Nonattribution of sources is a key component of an assessment. An assessment is focused on assisting an organization establish and define it's information security posture, rather than establishing fault of a specific individual for any discovered shortcoming.

Evaluation

An evaluation implies the use of hands-on technical means such as scanners, scripts, or other automated tools to reinforce or disprove the findings of the assessment. Occasionally, though, passive scanning may be used in an assessment to validate client-provided documentation such as network diagrams. "Penetration testing" or "Red Teaming" is not considered a part of basic system evaluation, but is a separate and more intense, usually non-cooperative testing of the target systems. There is a proposed NSA-Infosec Evaluation Methodology to be released in the near future. The author of this practical is not certified by NSA to practice this as yet unreleased IEM and all technical evaluation practices and procedures described in this paper are derived from other sources.

Audit

An audit, for the purpose of this exercise, implies that an external or internal authority has requested a formal check for compliance to various established standards, often bringing consequences to individuals responsible for adherence to the standards. This can create an adversarial relationship between auditor and audited that will not exist in an assessment situation. This distinction should be clarified with client's staff at the earliest possible opportunity in order to facilitate cooperation. Unfortunately, the negative connotations of the term "audit" have been deeply ingrained in the modern information technology culture.

Demonstration or Evaluation?

A demonstration, in this context, is a hands-off method of control validation where the assessor observes the performance of a procedure in order to verify information gained from interviews or existing documentation. This "over the shoulder" observation can provide insight into the "real world" operational activities of the target. Evaluation, as stated above, implies the use of additional technical means to validate control implementations.

[2] Miles, Greg; Rogers, Russ Et Al. "Security Assessment:
“Case Studies for Implementing the NSA-IAM".
Rockland, Mass. Syngress Publishing, Inc. 2004, pp 54-55

In this exercise, the author will be using the NSA-IAM to establish the target organization's infosec posture. The results of the assessment will identify areas in need of technical evaluation. Various techniques, including those taught in the SANS Auditing Systems, Networks, and Perimeters bootcamp will be used to evaluate these identified areas against both the target organization's information security policies, written or unwritten, and against industry established best practice.

Assignment 1: Research in Audit, Measurement, and Control

Introduction

To satisfy the requirements of Assignment 1 the author will research sources describing the current state of best practice regarding the evaluation of systems, components, and practices in use in order to facilitate the satisfactory completion of subsequent assignments.

Information Security Assessment

The United States Government National Security Agency's Information Security Assessment Methodology (NSA-IAM) is a non-intrusive means of analyzing an organization's information security posture. The full IAM checklist will be created for Assignment 2 and the results of the assessment will be presented in Assignment 3. Some of the questions raised by the initial assessment will be used in the construction of Assignment 2 technical evaluation checklists in order to further illuminate indicated areas of concern.

System Identification

The hardware component of the assessment is an Apple Computer Corporation Macintosh PowerBook laptop system featuring a single Power PC G4 (v3.2) processor running at 1 GHz clock speed with 1 GB main memory. It is configured with a 60Gb ATA hard drive and a CD/RW DVD/RW removable media SuperDrive. Connectivity options include built in 10/100/1000 Ethernet, 802.11b "Airport" wireless interface, a V.92 internal USB modem and the occasional use of a Verizon LG 4400B cell phone as a means of connecting to the Internet. External ports include 2 USB v1.1 ports and 1 400Mb Firewire port, along with SVGA, DVI, and Audio ports. The most critical software component in a computer system is the operating system. The current Apple offering, OS X version 10.3.3, is a BSD derived descendant of the defunct NEXT computer company's NEXTSTEP operating system which combines a mature GUI which benefits from many years of development effort with a well established and understood UNIX based system[3].

Potential Risks

Potential risks to the information contained in this target system consist of the following:

Loss of availability of data due to hardware malfunction is always a possibility in any system. These risks are increased in a portable system that is subjected to the physical stress of constant relocation. Potential consequences of hardware failure are the loss of use of the system while it is undergoing repairs, and loss of data if a failure occurred without proper information backup.

[3] 4 Reference.net
"Mac OS X History"
URL: http://www.4reference.net/encyclopedias/wikipedia/Mac_OS_X_history.html

The loss of the entire laptop system due to theft is always a possibility that demands constant vigilance on the part of the system owner. This would be an event of most severe consequence to the system owner due to loss of data availability, loss of use of the machine, and the expense of replacing a relatively expensive system.

Loss or corruption of data due to operator error is a risk of lesser probability due to the experience of the system owner, but is always a greater than zero possibility. This type of loss would be embarrassing, but ultimately recoverable.

Loss of control over system or compromise of information confidentiality, integrity, or availability due to unauthorized activities of third parties would also be extremely embarrassing to an information security professional, not to mention the potential for "real" losses, and also is a risk of greater than zero possibility.

Standards of Practice

In order to conduct a thorough evaluation it is necessary to refer to various sources to review the generally accepted standard of practice regarding system configuration and operational procedures. The following sources will be used to build the checklists for the technical evaluation portion of this exercise.

Sources for Standards of Practice for Apple OS X configuration and usage

For this exercise the opinions offered in the book "Mac OS X Maximum Security " by John and William C. Ray, along with suggestions offered in the SANS Institute Track 7 Auditing Networks, Perimeters and Systems 7.6 Advanced System Audit: UNIX workbook and other course material will be considered to be effective practices.

The author will be using a self-modified version of the latest OS X checklist from the NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION
INFORMATION SYSTEMS SECURITY OFFICE
"Risk Assessment/Countermeasure Analysis/Security Test and Evaluation (ST&E) for Mac OS X (Version 10.1 or later) Computer Systems"
Version 1.0 January 3, 2002
URL: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_macOSX.html

and the vulnerability evaluation tool
MacAnalysis from
Lagoon Software
URL: http://www.macanalysis.com/about.php3
to evaluate the OS X system configuration.

The SANS Top 10 Vulnerabilities list will also provide items for consideration.
URL: http://www.sans.org/top20/

The OS X section of the Occam's Razor website written by
Leon Towns-von Stauber
"Security"
Occam's Razor Mac OS X Presentations:
URL: http://www.occam.com/ocr/osx/
provides a thorough explanation of OS X security features.

Sources for Standards of Practice for Evaluation of Traffic Controls
Apple OS X includes an implementation of the traditional UNIX packet filter "ipfw" which is described in the system man pages and by
Chris Cochella in the article
"Configuring Jaguar's Firewall"
O' Reilly MacDevCenter.com
12/27/2002
URL: http://www.macdevcenter.com/pub/a/mac/2002/12/27/macosx_firewall.html

Firewall operations and evaluation procedures are described in the workbooks from the SANS Institute Track 7 Auditing Networks, Perimeters and Systems "Auditing the Perimeter", "Network Auditing Essentials", and by
Craig Robertson in the
GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.8
"Securing GIAC Enterprises FreeBSD as a Firewall Platform"
SANS InfoSec Reading Room.
6 January 2003
URL: http://www.giac.org/practical/GCFW/Craig_Robertson_GCFW.pdf

Sources for Standards of Practice for Evaluation of Logging and Auditing
The Apple OS X event logging system is based on the well-documented UNIX derived "syslog" utility. In addition to the system "man" pages, syslog history and secure usage is discussed in the paper published in the SANS InfoSec Reading Room titled "A Security Analysis of System Event Logging with Syslog" by Kenneth E. Nawyn, June 27, 2003.
URL: http://www.sans.org/rr/papers/index.php?id=1101

Logging considerations discussed in the SANS Institute Track 7 Auditing Networks, Perimeters and Systems course will also be included in the evaluation. A modified version of the freely available shell script based log analyzer "logcheck" is used to examine system logs for interesting events.
Instructions for use of this utility are found in articles by:
Marius Schamschula
"How to Configure logcheck Under Mac OS X"
Version 1.2.5 - 20021124
URL: http://www.hmug.org/HowTos/logcheck.html
and by
Trevor Warren
"Intrusion Detection Systems, Part IV: Logcheck"
freeos.com
URL: http://www.freeos.com/articles/3540/

Assignment 2: Create Plans and Checklists

Introduction

In Assignment 2 the author will construct a series of plans and checklists designed to assess and evaluate the target system in a structured manner using material from both the sources described in Assignment 1 and from personal experience.

Time Based Security[4]

Some of the concepts presented by Winn Schwartau in his book titled "Time Based Security" will be used to generate questions for the assessment. "How long" a particular control is effective is a major assessment criterion, as are event detection and staff reaction times.

Synopsis and interpretation of the NSA-IAM in outline form

An Information Security Assessment enables the assessor and the client to cooperatively answer the following six basic questions

1. Which information is most critical to the organization?
2. Which systems process, store, or transmit the critical information?
3. What are the operational processes involved in the processing, storage and/or transmission of the critical information?
4. What is the appropriate information security posture for the identified systems?
5. What are the potential system vulnerabilities?
6. What are the potential solutions to remediate or eliminate any identified vulnerabilities in the most cost effective manner?

A formal Information Security Assessment consists of three phases. The goals of each phase are explained in the following section.

1. Pre-Assessment Activities

- Client coordination, including but not limited to
    - Determining the client's goals and objectives
    - Setting the scope of the assessment
    - Obtaining relevant system documentation, if any
    - Dealing with logistical necessities, such as clearances, travel arrangements, coordination of meetings
    - Other client expectation issues
        - What are the client's existing security goals, if any?
        - Are there any specific legalities involved?

[4] Schwartau, Winn. "Time Based Security"
Interpact/Network Associates Special Edition 2nd printing May, 2001

- Information criticality assessment
  - What are the client's mission, goals and objectives?
  - What information is critical to the client's mission, goals and objectives?
  - What is the client's perception of which information is critical to the client's mission, goals and objectives?
  - What are the budgetary limitations?
- System Identification
  - Collection of available documentation
  - Determine logical and physical boundaries
  - Identify potential countermeasure constraints
    - User resistance to procedures
    - Potential performance degradations
- Write a technical assessment plan and checklist
- Include the following
  - Points of contact
  - Client's mission
  - Client's concerns
  - Information categories and criticality
  - Configuration diagrams for logical and physical hardware, software and communications entities
  - Documentation review, including a list of all reviewed system and organizational documents
  - Other team members (possibly subcontractors) with expertise in indicated specific areas of need
    - Attorney
    - Additional technical consultant
  - Pre-assessment summary & timeline
    - Who, What, Where, When, Why, How, How Long?

2. On-Site Activities

- Confirm findings and conclusions from Pre-Assessment phase
- Perform data gathering and validation of gathered data
  - Meetings
    - Get to know client(s)
    - Make sure client is clear about the process
    - Emphasize assessment rather than audit/inspection
    - Finalize the scope of the assessment
  - Interviews
  - Documentation review (lack of documentation is a finding)
  - System demonstrations
  - Technical evaluation, if indicated and allowed
    - Unobtrusive passive scanning of network to validate client provided documentation
- Provide an initial cursory analysis and feedback to client
  - Disclose any severe exposures immediately

3. Post-Assessment Activities
Final analysis
Prepare final report

For the purpose of this exercise, considering that the assessor and the client are the same entity, the distinction between the three formal phases will be blurred and some of the steps may be omitted. The "Post-Assessment Activities" called for in phase three will be presented in Assignment 4 of this practical.

Information Inventory and Classification

The system in question has, as most computing systems have, data, hardware, software, and operational components. The most valuable component of the system, in this writer's opinion, is the data contained in the system. After all, without information to process there would be very little point in maintaining expensive hardware and software or performing complex and potentially time-consuming operational procedures. A primary task in an information security assessment will be to identify and classify the various types of data to be protected.

In order to accurately determine information criticality, it is first necessary to perform a complete and accurate inventory of the data in question. This step in the process is essential in performing a valid information security assessment. It is impossible to adequately protect information if we do not know precisely what and where the information is. Defining information criticality is a crucial, if not the principal task in performing a successful infosec assessment. If we cannot completely inventory the information in question, there is no possibility of providing complete assurance. In addition, in a world bounded by limited budgets, it is essential to establish which information is most valuable to an organization so that finite resources can be effectively allocated.

Information Inventory and Classification Tasks

> *Information Criticality before System Criticality.*
> *The NSA-IAM is designed to identify the information criticality before the system criticality with a specific intent in mind. Each entity has a mission that it strives to achieve on a daily basis. This is the entity's reason for existence. Within that organization, there are specific pieces of information without which the organization will not be able to achieve its mission goals. By identifying those pieces of information first, we can better isolate the most critical systems within the organization. Without that information, we're left to try to defend every system component within the organization at the same level, which is not only inefficient but also wastes valuable time and resources.*[5]

[5] Miles and Rogers p 121

Describe the information in use by the organization in a logical sense without regard to the actual physical location of the data. First, list all the possible data types in use. Then, weed out the information that is not critical to the client's mission, if any. The data then will be grouped into as few broad groups as is reasonable. Classify and evaluate the criticality of the information in terms of agreed upon "impact attributes", including any possible time sensitivities. Interviewing the data owner(s), and then rating the data in terms of “impact attributes” and “impact definitions” will accomplish this task. From this evaluation of data, we will construct an organizational information criticality matrix to assist in the evaluation of potential risks.

Impact Attributes and Impact Definitions

Information is rated in terms of "impact attributes" and "impact definitions" in order to assess the value to the organization. The traditional impact attributes are the "CIA Triad", Confidentiality, Integrity, and Availability. It is certainly permissible to add additional impact attributes such as nonrepudiation or accountability, but there is an associated increase in complexity. In this exercise, the impact definitions "High", "Medium", and "Low" will be used, with "High" signifying a loss that would cause the organization's function to be severely impaired, "Medium" indicating a lesser inconvenience, and "Low" consisting of mere annoyance. Another possibility that provides consideration for the diverse opinions of a larger organization is to have each client representative numerically rate each data type in terms of impact and then calculate an average. The "high water mark" is the highest level rating for each impact attribute and is a requirement of the NSA-IAM. The "high water mark" is intended to provide the client with a feeling for which attributes are the most important. It is extremely important to remember that all the organization's information is valuable and to not regard data with lower impact ratings as non-essential. In addition, the tendency to confuse applications and systems with the data that is to be protected should be minimized.

Information Criticality

In order to effectively communicate the relative importance of different data types, the IAM requires construction of a box matrix, with the data descriptions listed in the row headers, and the columns headed by the agreed upon impact attributes. Each data type is associated with an impact definition for each impact attribute, and the impact definition is entered into the appropriate cell of the matrix. This exercise helps in visualizing the value of different information when attempting to prioritize protection efforts and is one of the most important IAM tasks.

System Criticality

Define the data in terms of the actual location of the data in the system's directory structure. First interviewing the owner of the data, and then documenting the actual location of the various data files will accomplish this goal. It will be necessary in this portion of the assessment to define both physical and logical boundaries between the various systems in question. Then we construct another matrix for each system or network device involved to help visualize the relative importance of different hosts and networks. Once the actual location and transmission path of the most valuable information is determined, it is necessary to establish priorities and to construct specific evaluation checklists for the indicated critical systems and network access points.

Cultural and Security Environment

In order to effectively perform a useful infosec assessment it is necessary to understand both the people who work in the entity to be assessed and their perceptions of how things either are done or "should be" done. This is the "cultural environment". It also is necessary to understand the existing policies, written and unwritten and any externally imposed regulatory requirements. This, in terms of the NSA-IAM, is the "security environment". The importance of understanding the corporate culture of the entity under assessment cannot be overemphasized. Organizational concerns and possible constraints need to be considered in the highest regard in order to provide an effective and useful assessment.

Technical Assessment Plan

In order to comply with the NSA-IAM there are nine specific areas comprising the TAP that must be considered and documented.[6]

1. Point of Contact
2. Organizational Mission
3. Organizational Information Criticality
4. System Informational Criticality
5. Client concerns and constraints
6. System Configuration
7. Interviews
8. Documentation
9. Timeline of Events

These nine areas must be included for NSA-IAM compliance, but other areas may be added as needed. Some of these areas will be omitted from this particular exercise due to lack of relevance in this particular situation.

The NSA-IAM requires investigation of 18 baseline information security categories [7]

The following checklist of questions is designed to provide a starting point for this investigation. As these questions are answered, more questions will undoubtedly be raised. Some questions are relevant in more than one category.

[6] Miles & Rogers P.190

[7] United States Government National Security Agency
Infosec Assessment Training and Rating Program
"IAM 18 Baseline INFOSEC Categories"
URL: http://www.iatrp.com/iam18baseline.cfm

Management Aspects

1. INFOSEC Documentation

Does any information security related documentation exist?

Policies

Procedures

Standards of practice

Guidance/Requirements

Is the documentation up to date and accurate?

How and where is which policy, practice or process documented?

Who maintains the documentation for which policy, practice or process?

Under what controls?

Are any mandatory documentation standards being observed?

Who has power of approval over documentation standards?

Who is the organizational point of contact regarding documentation issues?

Are there any externally imposed standards or regulations regarding documentation?

If there are any externally imposed standards or regulations regarding documentation, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who monitors and enforces compliance with documentation policy?

By what means?

Are there any regularly scheduled status reports generated regarding documentation?

Who is responsible for generating these reports, if any?

Who are the recipients of these reports, if any?

Do currently implemented documentation policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented documentation policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any documentation policies and/or practices?

How can these obstacles be overcome?

2. INFOSEC Roles and Responsibilities

Do clearly defined roles and responsibilities regarding information security exist?

Senior Management

Operational Staff

User Community

If so, what are they?
Who has power of approval over infosec roles and responsibilities?
Who is the organizational point of contact regarding
    infosec roles and responsibilities?
Who is the owner of each piece of critical information?

3. Contingency Planning

What contingency plans are available, written or unwritten, if any?
Who has power of approval over contingency plans?
Who is the organizational point of contact regarding
    contingency planning issues?
Who wrote the plan?
When was it last reviewed and/or updated?
How often is the plan tested?
When was the plan last tested?
What were the test results?
Who implements which parts of the plan?
Who updates the plan?
Under what circumstances is the plan updated?
What consideration is given to test results when updating plans?
How and where is the plan documented?
Is the documentation up to date and accurate?
Who maintains the documentation for the plan?
    Under what controls?
Where is the location of recovery facilities, if any?
What is the extent of any external recovery facilities?
What is the prioritization of essential functions to be restored in the
    event of an actual emergency?
Are any mandatory contingency planning standards being
    observed?
Are there any externally imposed standards or regulations
    regarding contingency planning?
If there are any externally imposed standards or regulations
    regarding contingency planning, are these standards being
        complied with?
    How is compliance being monitored and enforced?
    If not, are there plans to reach compliance?
    If not in compliance, has an official variance been granted?
    What is the duration of the variance, if any?
    What is the status of the compliance effort?
Are there any regularly scheduled status reports generated
        regarding contingency planning?
    Who is responsible for generating these reports, if any?
    Who are the recipients of these reports, if any?
Do currently implemented contingency planning policies and
    practices, if any, meet the current and future needs of the
        organization?
If not, how can these policies and/or practices be improved?

Are currently implemented contingency planning policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any contingency planning policies and/or practices?
How can these obstacles be overcome?

4. Configuration Management

What configuration management policies and procedures are in force, if any?
What undocumented configuration management practices are in use, if any?
Who defines configuration management policies and procedures?
Who implements configuration management policies and procedures?
Who monitors and enforces compliance with configuration management policies and procedures?
By what means?
Who has power of approval over configuration management policies and procedures?
Who is the organizational point of contact regarding configuration management issues?
How and where are configuration management policies and procedures documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
Under what controls?
Are any mandatory configuration management standards being observed?
Are there any externally imposed standards or regulations regarding configuration management?
If there are any externally imposed standards or regulations regarding configuration management, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?
What is the duration of the variance, if any?
What is the status of the compliance effort?
Are there any regularly scheduled status reports generated regarding configuration management?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?
Do currently implemented configuration management policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented configuration management policies and practices, if any, subject to periodic review?
If so, by whom?

What potential obstacles could inhibit timely improvement of any configuration management policies and/or practices?
How can these obstacles be overcome?

Technical Aspects

5. Identification and Authentication

What identification and authentication policies and procedures are in use, if any?
What undocumented practices are in use regarding identification and authentication, if any?
Who defines the identification and authentication policies and procedures?
Who has power of approval over identification and authorization policies and procedures?
Who is the organizational point of contact regarding identification and authentication issues?
Are any mandatory identification and authentication standards being observed?
Are there any externally imposed standards or regulations regarding identification and authentication?
If there are any externally imposed standards or regulations regarding identification and authentication, are these standards being complied with?
- If not, are there plans to reach compliance?
- If not in compliance, has an official variance been granted?
- What is the duration of the variance, if any?
- What is the status of the compliance effort?

Who implements identification and authentication policies and procedures?
Who monitors and enforces compliance with identification and authentication policies and procedures
- By what means?

How and where are identification and authentication policies and procedures documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
- Under what controls?

Are there any regularly scheduled status reports generated regarding identification and authentication?
- Who is responsible for generating these reports, if any?
- Who are the recipients of these reports, if any?

Are there any automatic protection mechanisms enforcing the identification and authentication process?
- If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case.

Have existing automatic protection mechanisms been tested?
- When was the last test?
- Who performed the test?
- What was the test procedure?
- What were the expected results?
- What were the actual results?
- What is the potential maximum duration of exposure?
- What is the cost potential of maximum duration of exposure?
- What is the minimum detectable duration of exposure?
- What were the measured protection, detection and response times of control systems?
- Within operational constraints, if any, how can protection time be increased?
- Within operational constraints, if any, how can detection time and/or response time be decreased?
- How are test results taken into consideration when forming or adjusting identification and authentication policies?

Do currently implemented identification and authorization policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented identification and authentication policies and practices, if any, subject to periodic review?
- If so, by whom?

What potential obstacles could inhibit timely improvement of any identification and authorization policies and/or practices?

How can these obstacles be overcome?

6. Account Management

What account management policies and procedures are in use, if any?

What undocumented account management practices are in use, if any?

Who defines the account management policies and procedures?

Who has power of approval over account management policies and procedures?

Who is the organizational point of contact regarding account management issues?

Are any mandatory account management standards being observed?

Are there any externally imposed standards or regulations regarding account management?

If there are any externally imposed standards or regulations regarding account management, are these standards being complied with?
- If not, are there plans to reach compliance?
- If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?
What is the status of the compliance effort?
Who implements account management policies and procedures?
Who monitors and enforces compliance with account management policies and procedures
By what means?
How and where are account management policies and procedures documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
Under what controls?
Are there any regularly scheduled status reports generated regarding account management?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?
Are there any automatic protection mechanisms enforcing the account management process?
If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..
Have existing automatic protection mechanisms been tested?
When was the last test?
Who performed the test?
What was the test procedure?
What were the expected results?
What were the actual results?
What is the potential maximum duration of exposure?
What is the cost potential of maximum duration of exposure?
What is the minimum detectable duration of exposure?
What were the measured protection, detection and response times of control systems?
Within operational constraints, if any, how can protection time be increased?
Within operational constraints, if any, how can detection time and/or response time be decreased?
How are test results taken into consideration when forming or adjusting account management policies?
Do currently implemented account management policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented account management policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any account management policies and/or practices?

How can these obstacles be overcome?

7. Session Controls

What session control policies and procedures are in use, if any?
What undocumented session control practices are in use, if any?
Who defines the session control policies and procedures?
Who has power of approval over session control policies and procedures?
Who is the organizational point of contact regarding session control issues?
Are any mandatory session control standards being observed?
Are there any externally imposed standards or regulations regarding session controls?
If there are any externally imposed standards or regulations regarding session controls, are these standards being complied with?
    If not, are there plans to reach compliance?
    If not in compliance, has an official variance been granted?
    What is the duration of the variance, if any?
    What is the status of the compliance effort?
Who implements session control policies and procedures?
Who monitors and enforces compliance with session control policies and procedures?
    By what means?
How and where are session control policies and procedures documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
    Under what controls?
Are there any regularly scheduled status reports generated regarding session controls?
    Who is responsible for generating these reports, if any?
    Who are the recipients of these reports, if any?
Are any automatic session control mechanisms implemented?
Have existing automatic session control mechanisms been tested?
    When was the last test?
    Who performed the test?
    What was the test procedure?
    What were the expected results?
    What were the actual results?
    What is the potential maximum duration of exposure?
    What is the cost potential of maximum duration of exposure?
    What is the minimum detectable duration of exposure?
    What were the measured protection, detection and response times of control systems?
    Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting session control policies?

Do currently implemented session control policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented session control policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any session control policies and/or practices?

How can these obstacles be overcome?

8. External Connectivity

Internet Usage

Is Internet usage permitted?

What Internet usage policies are in force, if any?

What undocumented Internet usage practices are in use, if any?

Who defines Internet usage policies?

Who has power of approval over Internet usage policies?

Who is the organizational point of contact regarding Internet usage security issues?

Are any mandatory Internet usage standards being observed?

Are there any externally imposed standards or regulations regarding Internet usage?

If there are any externally imposed standards or regulations regarding Internet usage, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements Internet usage policies and procedures?

Who monitors and enforces compliance with Internet usage policies and procedures?

By what means?

How and where are Internet usage policies and procedures documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding Internet usage?

- Who is responsible for generating these reports?
- Who are the recipients of these reports, if any?

Are Internet communications sessions encrypted?

- If so, by what means?
- Who is responsible for generating, maintaining, and distributing any encryption keys or certificates? Describe this process.

Are there any automatic protection mechanisms enforcing the Internet usage policy?

If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..

Have existing automatic protection mechanisms been tested?

- When was the last test?
- Who performed the test?
- What was the test procedure?
- What were the expected results?
- What were the actual results?
- What is the potential maximum duration of exposure?
- What is the cost potential of maximum duration of exposure?
- What is the minimum detectable duration of exposure?
- What were the measured protection, detection and response times of control systems?

Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting Internet usage policies?

Do currently implemented Internet usage policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented Internet usage policies and practices, if any, subject to periodic review?

- If so, by whom?

What potential obstacles could inhibit timely improvement of any Internet usage policies and/or practices?

How can these obstacles be overcome?

Modems

Is modem usage permitted?

What modem usage policies and procedures are in force, if any?

- What undocumented modem usage practices are in use, if any?
- Who defines the modem usage policies and procedures?
- Who has power of approval over modem usage policies?
- Who is the organizational point of contact regarding modem security issues?
- Are any mandatory modem usage standards being observed?
- Are there any externally imposed standards or regulations regarding modem usage?
- If there are any externally imposed standards or regulations regarding modem usage, are these standards being complied with?
  - If not, are there plans to reach compliance?
  - If not in compliance, has an official variance been granted?
  - What is the duration of the variance, if any?
  - What is the status of the compliance effort?
- Who implements the modem usage policies and procedures?
- How and where are modem usage policies and procedures documented?
- Is the documentation up to date and accurate?
- Who monitors and enforces compliance with the modem usage policies and procedures?
  - By what means?
- Who maintains the documentation for which processes?
  - Under what controls?
- Are there any regularly scheduled status reports generated regarding modem usage?
  - Who is responsible for generating these reports?
  - Who are the recipients of these reports, if any?
- Are modem based communications sessions encrypted?
  - If so, by what means?
  - Who is responsible for generating, maintaining, and distributing any encryption keys or certificates? Describe this process.
- Are there any automatic protection mechanisms enforcing the modem usage policy?
- If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..
- Have existing automatic protection mechanisms been tested?
  - When was the last test?

Who performed the test?

What was the test procedure?

What were the expected results?

What were the actual results?

What is the potential maximum duration of exposure?

What is the cost potential of maximum duration of exposure?

What is the minimum detectable duration of exposure?

What were the measured protection, detection and response times of control systems?

Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting modem usage policies?

Do currently implemented modem usage policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented modem usage policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any modem usage policies and/or practices?

How can these obstacles be overcome?

Dedicated Communication Lines

Are dedicated communication lines in use?

What policies and procedures regarding dedicated communication lines are in force, if any?

What undocumented practices are in use regarding dedicated lines, if any?

Who defines policies and procedures regarding dedicated communication lines?

Who has power of approval over dedicated line policies?

Who is the organizational point of contact regarding dedicated line security issues?

Are any mandatory dedicated communication line standards being observed?

Are there any externally imposed standards or regulations regarding dedicated communication lines?

If there are any externally imposed standards or regulations regarding dedicated communication lines, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?
What is the status of the compliance effort?

Who implements policies and procedures regarding dedicated communication lines?

Who monitors and enforces compliance with policies and procedures regarding dedicated communication lines?
By what means?

How and where are dedicated usage policies and procedures documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?
Under what controls?

Are there any regularly scheduled status reports generated regarding dedicated line usage?
Who is responsible for generating these reports?
Who are the recipients of these reports, if any?

Are transmissions over dedicated lines encrypted?
If so, by what means?
Who is responsible for generating, maintaining, and distributing any encryption keys or certificates?
Describe this process.

Are there any automatic protection mechanisms enforcing the dedicated line policy?

If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..

Have existing automatic protection mechanisms been tested?
When was the last test?
Who performed the test?
What was the test procedure?
What were the expected results?
What were the actual results?
What is the potential maximum duration of exposure?
What is the cost potential of maximum duration of exposure?
What is the minimum detectable duration of exposure?
What were the measured protection, detection and response times of control systems?

Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting dedicated line usage policies?

Do currently implemented dedicated line usage policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented dedicated line policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any dedicated line policies and/or practices?

How can these obstacles be overcome?

Wireless Connectivity

Is wireless usage allowed?

What policies and procedures regarding wireless connectivity are in force, if any?

What undocumented practices are in use regarding wireless connectivity, if any?

Who defines policies and procedures regarding wireless connectivity?

Who has power of approval over wireless usage policies?

Who is the organizational point of contact regarding wireless security issues?

Are any mandatory wireless usage standards being observed?

Are there any externally imposed standards or regulations regarding wireless usage?

If there are any externally imposed standards or regulations regarding wireless usage, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements policies and procedures regarding wireless connectivity?

Who monitors and enforces compliance with policies and procedures regarding wireless connectivity ?

By what means?

How and where are wireless connectivity usage policies and procedures documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding wireless usage?

Who is responsible for generating these reports?

  - Who are the recipients of these reports, if any?
- Are wireless sessions encrypted?
  - If so, by what means?
  - Who is responsible for generating, maintaining, and distributing any encryption keys or certificates?
  - Describe this process.
- Are there any automatic protection mechanisms enforcing any wireless connectivity policies?
- If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..
- Have existing automatic protection mechanisms been tested?
  - When was the last test?
  - Who performed the test?
  - What was the test procedure?
- What were the expected results?
- What were the actual results?
- What is the potential maximum duration of exposure?
- What is the cost potential of maximum duration of exposure?
- What is the minimum detectable duration of exposure?
- What were the measured protection, detection and response times of control systems?
- Within operational constraints, if any, how can protection time be increased?
- Within operational constraints, if any, how can detection time and/or response time be decreased?
- How are test results taken into consideration when forming or adjusting wireless usage policies?
- Do currently implemented wireless usage policies and practices, if any, meet the current and future needs of the organization?
- If not, how can these policies and/or practices be improved?
- Are currently implemented wireless usage policies and practices, if any, subject to periodic review?
  - If so, by whom?
- What potential obstacles could inhibit timely improvement of any wireless usage policies and/or practices?
- How can these obstacles be overcome?

9. Telecommunications

- What other telecommunications policies and procedures are in force, if any?
- What undocumented telecommunications practices are in use, if any?
- Who defines telecommunications policies and procedures?

Who has power of approval over telecommunications policies and procedures?

Who is the organizational point of contact regarding telecommunications security issues?

Are any mandatory telecommunications standards being observed?

Are there any externally imposed standards or regulations regarding telecommunications?

If there are any externally imposed standards or regulations regarding telecommunications, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements telecommunications policies and procedures?

Who monitors and enforces compliance with telecommunications policies and procedures?

By what means?

How and where are telecommunications policies and procedures documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding telecommunications security?

Who is responsible for generating these reports, if any?

Who are the recipients of these reports, if any?

Are telecommunications sessions encrypted?

If so, by what means?

Who is responsible for generating, maintaining, and distributing any encryption keys or certificates?

Describe this process.

Are there any automatic protection mechanisms enforcing the telecommunications policies?

If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case.

Have existing automatic protection mechanisms been tested?

When was the last test?

Who performed the test?

What was the test procedure?

What were the expected results?

What were the actual results?

What is the potential maximum duration of exposure?

What is the cost potential of maximum duration of exposure?

What is the minimum detectable duration of exposure?

What were the measured protection, detection and response times of control systems?

Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting telecommunications usage policies?

Do currently implemented telecommunications policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented telecommunications policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any telecommunications policies and/or practices?

How can these obstacles be overcome?

10. Logging and Auditing

What logging and audit policies and procedures are in force, if any?

What undocumented practices are in use regarding logging and/or auditing, if any?

Who defines logging and audit policies and procedures?

Who has power of approval over logging and auditing policies and procedures?

Who is the organizational point of contact regarding logging and auditing issues?

Are any mandatory logging and audit standards being observed?

Are there any externally imposed standards or regulations regarding logging and auditing?

If there are any externally imposed standards or regulations regarding logging and auditing, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements logging and audit policies and procedures?

Who monitors and enforces compliance with logging and audit policies and procedures?

By what means?

How and where are logging and audit policies and procedures documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding logging and auditing?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?
Are logs and log transmissions encrypted?
If so, by what means?
Who is responsible for generating, maintaining, and distributing any encryption keys or certificates?
Describe the process.
Have existing logging and auditing mechanisms been tested?
When was the last test?
Who performed the test?
What was the test procedure?
What were the expected results?
What were the actual results?
How are test results taken into consideration when forming or adjusting logging and auditing policies?
Do currently implemented logging and auditing policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented logging and auditing policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any logging and auditing policies and/or practices?
How can these obstacles be overcome?

11. Virus/Malware Protections

What policies and procedures are in force regarding virus/malware protections, if any?
What undocumented practices are in use regarding virus/malware protection, if any?
Who defines policies and procedures regarding virus/malware protections?
Who has power of approval over malicious software control policies and procedures?
Who is the organizational point of contact regarding malicious software control issues?
Are any mandatory standards regarding potentially malicious software programs being observed?
Are there any externally imposed standards or regulations regarding potentially malicious software programs?
If there are any externally imposed standards or regulations regarding potentially malicious software programs, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements policies and procedures regarding virus/malware protections?

Who monitors and enforces compliance with policies and procedures regarding virus/malware protections?

By what means?

How and where are policies and procedures regarding virus/malware protections documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding malicious code abatement?

Who is responsible for generating these reports, if any?

Who are the recipients of these reports, if any?

Are there any automatic protection mechanisms performing the virus/malware control process?

If so, describe those mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..

Have existing automatic protection mechanisms been tested?

When was the last test?

Who performed the test?

What was the test procedure?

What were the expected results?

What were the actual results?

What is the potential maximum duration of exposure?

What is the cost potential of maximum duration of exposure?

What is the minimum detectable duration of exposure?

What were the measured protection, detection and response times of control systems?

Within operational constraints, if any, how can protection time be increased?

Within operational constraints, if any, how can detection time and/or response time be decreased?

How are test results taken into consideration when forming or adjusting malware control policies?

Do currently implemented malicious code control policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented malicious code control policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any malicious code control policies and/or practices?
How can these obstacles be overcome?

12. Maintenance Activities

What policies and procedures are in force regarding maintenance activities, if any?
What undocumented practices are in use regarding maintenance activities, if any?
Who defines policies and procedures regarding maintenance activities?
Who has power of approval over maintenance activity policies and procedures?
Who is the organizational point of contact regarding system maintenance issues?
Are any mandatory standards regarding maintenance activities being observed?
Are there any externally imposed standards or regulations regarding maintenance activities?
If there are any externally imposed standards or regulations regarding maintenance activities, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?
What is the duration of the variance, if any?
What is the status of the compliance effort?
Who implements policies and procedures regarding maintenance activities?
Who monitors and enforces compliance with policies and procedures regarding maintenance activities?
By what means?
How and where are policies and procedures regarding maintenance activities documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
Under what controls?
Are there any regularly scheduled status reports generated regarding system maintenance activities?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?
Are there any automatic mechanisms performing maintenance activities?
If so, describe those mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations.
Have existing automatic mechanisms been tested?
When was the last test?
Who performed the test?

What was the test procedure?
What were the expected results?
What were the actual results?
How are test results taken into consideration when forming or adjusting maintenance policies?
Do currently implemented system maintenance policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented system maintenance policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any system maintenance policies and/or practices?
How can these obstacles be overcome?

13. Backup/Recovery

What backup/recovery policies and procedures are in force, if any?
What undocumented backup and recovery practices are in use, if any?
Who defines backup/recovery policies and procedures?
Who has power of approval over backup and recovery policies and procedures?
Who is the organizational point of contact regarding backup and recovery issues?
Are any mandatory backup standards being observed?
Are there any externally imposed standards or regulations regarding backup and recovery procedures?
If there are any externally imposed standards or regulations regarding backup and recovery procedures, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?
What is the duration of the variance, if any?
What is the status of the compliance effort?
Who implements backup/recovery policies and procedures?
Who monitors and enforces compliance with backup/recovery policies and procedures?
By what means?
How and where are policies and procedures documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
Under what controls?
Are there any regularly scheduled status reports generated regarding backup and recovery?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?

Are backup processes encrypted?
If so, by what means?
Who is responsible for generating, maintaining, and distributing any encryption keys or certificates?
Describe this process.
When was the last restoration drill?
What was the extent of the restoration drill?
What were the results of the restoration drill?
What was learned as a result of the restoration drill?
Were any results of a restoration drill used as a justification to modify backup policy?
Are original backup media or copies stored offsite?
If so, where?
If offsite media storage is under control of outside entity, what is the name of the company and who is the point of contact?
What is the contact procedure?
What is the procedure for sending media offsite?
What is the procedure for recovering media from offsite storage?
Is there an expedited recovery procedure for emergencies?
Who is the organizational point of contact regarding offsite storage issues?
Do currently implemented backup and recovery policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented backup and recovery policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any backup and recovery policies and/or practices?
How can these obstacles be overcome?

Operational Aspects

14. Labeling/Classification of data

What policies and procedures are in force regarding labeling/classification of data, if any?
What undocumented practices are in use regarding labeling/classification of data, if any?
Who defines policies and procedures regarding labeling/classification of data?
Who has power of approval over data classification policies and procedures?
Who is the organizational point of contact regarding data classification issues?
Are any mandatory data classification standards being observed?

Are there any externally imposed standards or regulations regarding data labeling or classification?

If there are any externally imposed standards or regulations regarding data labeling or classification, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements policies and procedures regarding labeling/classification of data?

Who monitors and enforces compliance with policies and procedures regarding labeling/classification of data?

By what means?

How and where are policies and procedures regarding labeling/classification of data documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding data labeling and classification?

Who is responsible for generating these reports, if any?

Who are the recipients of these reports, if any?

Are there any automatic protection mechanisms enforcing the labeling and classification of data?

If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations.

Have existing automatic protection mechanisms been tested?

When was the last test?

Who performed the test?

What was the test procedure?

What were the expected results?

What were the actual results?

How are test results taken into consideration when forming or adjusting data classification policies?

Do currently implemented data classification policies and practices, if any, meet the current and future needs of the organization?

If not, how can these policies and/or practices be improved?

Are currently implemented data classification policies and practices, if any, subject to periodic review?

If so, by whom?

What potential obstacles could inhibit timely improvement of any data classification policies and/or practices?

How can these obstacles be overcome?

15. Media sanitization and disposal

- What policies and procedures are in force regarding media sanitization and disposal, if any?
- What undocumented media sanitation and disposal practices are in use, if any?
- Who defines policies and procedures regarding media sanitization and disposal?
- Who has power of approval over media sanitization and disposal policies and procedures?
- Who is the organizational point of contact regarding media sanitization and disposal issues?
- Are any mandatory media disposal standards being observed?
- Are there any externally imposed standards or regulations regarding media disposal?
- If there are any externally imposed standards or regulations regarding media disposal, are these standards being complied with?
    - How is compliance being monitored and enforced?
    - If not, are there plans to reach compliance?
    - If not in compliance, has an official variance been granted?
    - What is the duration of the variance, if any?
    - What is the status of the compliance effort?
- Who implements policies and procedures regarding media sanitization and disposal?
    - Who monitors compliance with policies and procedures regarding media sanitization and disposal?
    - By what means?
- How and where are policies and procedures regarding media sanitization and disposal documented?
- Is the documentation up to date and accurate?
- Who maintains the documentation for which processes?
    - Under what controls?
- Are there any regularly scheduled status reports generated regarding media sanitization and disposal?
    - Who is responsible for generating these reports, if any?
    - Who are the recipients of these reports, if any?
- Do currently implemented media control policies and practices, if any, meet the current and future needs of the organization?
- If not, how can these policies and/or practices be improved?
- Are currently implemented media control policies and practices, if any, subject to periodic review?
    - If so, by whom?
- What potential obstacles could inhibit timely improvement of any media control policies and/or practices?
- How can these obstacles be overcome?

16. Physical security

What policies and procedures are in force regarding physical security, if any?

What undocumented physical security practices are in use, if any?

Who defines policies and procedures regarding physical security?

Who has power of approval over physical security policies and procedures?

Who is the organizational point of contact regarding physical security issues?

Are any mandatory physical security standards being observed?

Are there any externally imposed standards or regulations regarding physical security?

If there are any externally imposed standards or regulations regarding physical security, are these standards being complied with?

If not, are there plans to reach compliance?

If not in compliance, has an official variance been granted?

What is the duration of the variance, if any?

What is the status of the compliance effort?

Who implements policies and procedures regarding physical security?

Who monitors and enforces compliance with policies and procedures regarding physical security?

By what means?

How and where are policies and procedures regarding physical security documented?

Is the documentation up to date and accurate?

Who maintains the documentation for which processes?

Under what controls?

Are there any regularly scheduled status reports generated regarding physical security?

Who is responsible for generating these reports, if any?

Who are the recipients of these reports, if any?

Are there any automatic protection mechanisms enforcing the physical security policies?

If so, describe the protection mechanisms, including any means used to detect variance from policy and any practices designed to react to policy violations. Also, describe the expected protection, detection and reaction times, best case and worst case..

Have existing automatic protection mechanisms been tested?

When was the last test?

Who performed the test?

What was the test procedure?

What were the expected results?

What were the actual results?

What is the potential maximum duration of exposure?

What is the cost potential of maximum duration of exposure?

What is the minimum detectable duration of exposure?
What were the measured protection, detection and response times of control systems?
Within operational constraints, if any, how can protection time be increased?
Within operational constraints, if any, how can detection time and/or response time be decreased?
How are test results taken into consideration when forming or adjusting usage policies?

Do currently implemented physical security policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented physical security policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any physical security policies and/or practices?
How can these obstacles be overcome?

17. Personnel Security

What policies and procedures are in force regarding personnel security issues, if any?
What undocumented personnel security practices are in use, if any?
Who defines policies and procedures regarding personnel security issues?
Who has power of approval over personnel security policies and procedures?
Who is the organizational point of contact regarding personnel security issues?
Are any mandatory personnel security standards being observed?
Are there any externally imposed standards or regulations regarding personnel security?
If there are any externally imposed standards or regulations regarding personnel security, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?
What is the duration of the variance, if any?
What is the status of the compliance effort?
Who implements policies and procedures regarding personnel security issues?
Who monitors and enforces compliance with policies and procedures regarding personnel security issues?
By what means?
How and where are policies and procedures regarding personnel security issues documented?

Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
Under what controls?

Are there any regularly scheduled status reports generated regarding personnel security issues?
Who is responsible for generating these reports, if any?
Who are the recipients of these reports, if any?
Are there any "key" persons whose loss due to job change, retirement, or accidental incapacitation would impact system operations or information security?
Are personnel background and/or reference checks performed?
Do currently implemented personnel security policies and practices, if any, meet the current and future needs of the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented personnel security policies and practices, if any, subject to periodic review?
If so, by whom?
What potential obstacles could inhibit timely improvement of any personnel security policies and/or practices?
How can these obstacles be overcome?

18. Training and security awareness

What policies and procedures are in force regarding training and security awareness, if any?
What undocumented practices are in use regarding training and security awareness, if any?
Who defines policies and procedures regarding training and security awareness?
Who has power of approval over training and security awareness policies and procedures?
Who is the organizational point of contact regarding training and security awareness issues?
Are any mandatory training and security awareness standards being observed?
Are there any externally imposed standards or regulations regarding training and security awareness?
If there are any externally imposed standards or regulations regarding training and security awareness, are these standards being complied with?
If not, are there plans to reach compliance?
If not in compliance, has an official variance been granted?
What is the duration of the variance, if any?
What is the status of the compliance effort?
Who implements policies and procedures regarding training and security awareness?

Who monitors and enforces compliance with policies and
    procedures regarding training and security awareness?
        By what means?
How and where are policies and procedures regarding
    training and security awareness documented?
Is the documentation up to date and accurate?
Who maintains the documentation for which processes?
    Under what controls? .
Are there any regularly scheduled status reports generated
        regarding training and security awareness?
    Who is responsible for generating these reports, if any?
    Who are the recipients of these reports, if any?
Are any persons "cross trained" to assume the responsibilities of
others in case of necessity?
Do currently implemented training and security awareness policies
    and practices, if any, meet the current and future needs of
    the organization?
If not, how can these policies and/or practices be improved?
Are currently implemented training and security awareness policies
    and practices, if any, subject to periodic review?
        If so, by whom?
What potential obstacles could inhibit timely improvement of any
    training and security awareness policies and/or practices?
How can these obstacles be overcome?

Some of these questions may on the surface appear to be redundant. This is by design and the intent is to construct a checklist that will be useful in a variety of different situations. Of course, additional categories may be defined as desired by the assessor and the client. Additional categories may raise additional assessment questions. The practice of "outsourcing" comes to mind as an additional potential assessment category, but will not be included in this exercise.

Technical evaluation plans
These items have been identified by the answers provided for the IAM checklist as being in need of further clarification by technical evaluation.
The plans will be executed for Assignment 3.

OS X configuration and usage
Network traffic control
Logging and event reporting

Plan for assessment and evaluation of OS X configuration and usage
Modify Naval Surface Warfare Center audit checklist [8]
(original version omitted from this report for considerations of length)
Add additional checklist items as needed
Include the following considerations for each checklist item:

- References
- Control Objectives
  - What is the control supposed to achieve?
- Control Description
- Potential Risks
  - What are the consequences of control failure?
- Compliance
  - How can we tell if the system is in compliance with the control?
- Verification of control
  - Demonstration or Evaluation?
- Residual risk
  - What risks remain in spite of properly functioning controls?

Answer modified checklist and record results for Assignment 3

- Interpret results.

Plan for Assessment and Evaluation of Network Traffic Control
Evaluation Objectives
Verify that the system network traffic control subsystem is correctly installed, appropriately configured for the organizational mission, and is operating as expected. Verify traffic is being passed or filtered as intended, and that notable events are logged to appropriate location.

List potential risks of firewall compromise

Firewall assessment plan

- What information is the firewall supposed to protect?
- What risks are acceptable?
- What change control is in effect?

Policy Evaluation

- Describe and examine use of ipfw rules taken from /etc/ipfw.conf.
  - Static or Stateful rules?
- Include the file "/etc/ipfw.conf"
- Describe rationale for each rule
- Verify ruleset is installed**.**

[8] NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION
INFORMATION SYSTEMS SECURITY OFFICE
“Risk Assessment/Countermeasure Analysis/Security Test and Evaluation (ST&E) for Mac OS X (Version 10.1 or later) Computer Systems”
Version 1.0 January 3, 2002
URL: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_macOSX.html

Firewall technical evaluation plan

Map open ports with nmap

(y.y.y.y = address of attack machine) (x.x.x.x = address of target machine)
Execute the following nmap commands, record results,
Observe system logging with "tail -f /var/log/system.log"
in shell window, note relevant entries.

```
/usr/local/bin/nmap -v -v -Tinsane -sT -O -p1-65000 x.x.x.x
```

This invocation will probe all ports on the target and record all results in verbose mode. The scan will include a TCP connect() scan and a OSScan to attempt to perform operating system fingerprinting.
The "insane" timing policy will invoke the most aggressive scans

```
/usr/local/bin/nmap -v -v -Tinsane -sU -O -p1-65000 x.x.x.x
```

This invocation will probe all ports on the target and record all results. The scan will include a UDP scan and a OSScan to attempt to perform operating system fingerprinting.
The "insane" timing policy will invoke the most aggressive scans

```
/usr/local/bin/nmap -v -v -Tinsane -sS -O -p1-65000 x.x.x.x
```

This invocation will probe all ports on the target and record all results. The scan will include a TCP SYN half-open stealth scan to attempt to avoid logging and a OSScan to attempt to perform operating system fingerprinting.
The "insane" timing policy will invoke the most aggressive scans

```
/usr/local/bin/nmap -v -v -Tinsane -g53 -sS -O -p1-65000 x.x.x.x
```

This invocation will probe all ports on the target and record all results. It will probe the target from port 53 in an attempt to simulate DNS traffic and record all resulting traffic. The scan will include a TCP SYN half-open stealth scan to attempt to avoid logging and a OSScan to attempt to perform operating system fingerprinting.
The "insane" timing policy will invoke the most aggressive scans

Perform the nmap scans listed above in the following test configurations.

Internal scan with firewall activated in normal operating mode.
Internal scan with firewall disabled to investigate active services.
(Security note: Unplug any active Internet connection while performing this test.)
Scan from external machine
Scan from external machine with firewall disabled for comparison, and to simulate firewall breakdown or penetration.
(Security note: Unplug any active Internet connection while performing this test. Connect systems with an isolated ethernet hub or crossover cable while firewall is disabled.)

Analyze results of nmap scans.

- What are the expected results of this test?
- Describe exposed services and other interesting results

Vulnerability scanning with nessus

scan the default range (nmap services + privileged ports) TCP/UDP ports using TCP connect() method.
Configure the scanner to use the most intense level of scanning

Perform the nessus scans in the same test configurations as for nmap.
Save scan results as ASCII text. Include scan reports as an appendix.

Analyze results of nessus scans including any observed event logging.

- What are the expected results of this test
- Describe exposed services and other interesting results

"Little Snitch"[9]

Control objective

- Describe expected behavior of outbound traffic filter.

Control description
What is the potential risk if this control fails?
Verify program function

- Attempt to invoke embedded URL from within this document:
- Verify appropriate logging and notification.

Verify logging by examining logs produced during firewall tests.

- Were all scans/probes detected and logged?
- Were any events missed?
- Were any logging thresholds reached?

Plan for Assessment and Evaluation of Logging Subsystem
Evaluation Objectives

Verify that implementation of system logging and event reporting are in conformance with the stated needs of the organization and are functioning as expected.

Describe potential risks of logging failures

Plan for examination of logging subsystem

Describe logging policy and expected behavior of logging subsystem:

- Examine /etc/syslog.conf.
- Verify that desired information is being logged to desired location by
  manual examination of logfiles using "tail -f /var/log/system.log"
- Trigger various reportable events and verify generation of log entries.

[9] Little Snitch Application Supervisor
Objective Development
URL: http://www.obdev.at/products/littlesnitch/index.html

Examine use of "logcheck" system log utility.

Describe expected behavior of log event reporting subsystem.

Verify program is automatically launched on appropriate schedule.

Verify notifications by visual inspection of mailbox. Do reports arrive at appropriate time?

Verify logcheck is correctly categorizing events by examination of mailed report

Verify appropriate archiving of logs and notifications by visual examination of log directory. Include sample directory listing

MacAnalysis[10]

Describe expected behavior of vulnerability assessment tool MacAnalysis

Run MacAnalysis against system

Interpret results.

Explain any difference in findings from the modified NSWC checklist and the MacAnalysis run.

Assessment of potential risk from the current SANS Top 10 UNIX vulnerabilities

Obtain latest UNIX vulnerability listing from SANS website

Assess system configuration in terms of these vulnerabilities.

[10] Lagoon Software
MacAnalysis vulnerability evaluation tool V.2.3X
URL: http://www.macanalysis.com/about.php3

Assignment 3: Conduct the Assessment and Evaluation

Introduction

In this section, the results of the assessment and evaluation proposed in Assignment 2 will be presented.

An Information Security Assessment consists of three phases

1. Pre-Assessment Activities

In a "real world" infosec assessment, pre-assessment activities would include a pre-assessment on-site visit (PASV) for the purpose of meeting with the client in order to gather information, establish client priorities and expectations, set the scope of the assessment, and gain awareness of the business goals of the client. This visit is intended to provide the assessor with adequate information to construct a first draft of the assessment plan, get a feel for the client's security environment, and to begin to build the information and system criticality matrices. In this particular instance, since assessor and client are the same entity, an actual PASV will not be necessary.

2. On-Site Activities

For this exercise, there is no difference between "off-site" and "on-site", so the boundaries between the formal phases in this case are at best, indistinct.

3. Post-Assessment Activities

Create final risk analysis and report, which will include specific recommendations for remediation or mitigation of potential exposure. The analysis will include references to any positive findings as well as any shortcomings. This report will be presented in Assignment 4.

Cultural and Security Environment

The client organization is a small information security consultancy that relies on the information contained in the target system in order to successfully perform business activities. The system owner is dedicated to keeping current with trends in the field, but is sometimes lax in applying the "state of the art" to his own personal system. There are no written security policies in place, but there is a considerable flexibility in implementing or changing practices due to extremely low bureaucratic overhead.

Technical Assessment Plan

1. Point of Contact
   Claude V. Lucas
2. Organizational Mission of target system(s)
   Personal use
3. Organizational Information Criticality
   Defined in Organizational Information Criticality Matrix
4. System Informational Criticality
   Not relevant in this situation. All critical data exists on single system.

5. Client concerns and constraints
   Client is concerned that the system is properly configured and updated (patched) in a timely manner, and that Internet usage does not increase the level of system vulnerability
6. System Configuration
   Apple PowerBook, 1Ghz, 1Gb RAM
   Apple OS X V10.3.3 MS Win2000/Virtual PC
7. Interviews
   Not needed in this instance, assessor and assessed are the same person
8. Documentation
   No formal documentation exists for this system
9. Timeline of Events.
   Tentative completion date 12-April-2004

An Information Security Assessment enables the assessor and the client to cooperatively answer the following six questions

1. Which information is most critical to the organization?

The client's data consists of
Email, current and archived
Contact information (address book)
Accounting data, both personal and business
Legal documents
Personal website pages
Audio files
  Downloaded
  Original
Photographs
System configuration data
  This system
  Other systems
Scripts and other personally written software
Study and reference materials
Research sources and findings
  Web bookmarks
Contents of Virtual PC virtual disk drive
Installed software registration serial numbers

Organizational Information Criticality Matrix

Type of Information	Confidentiality	Integrity	Availability
Email Correspondence, current and archived	High	High	Medium
Accounting data	High	High	Medium
Local website	Medium	Medium	Low
Original and other audio files	Medium	High	Medium
Photographs	Low	High	Medium
System configuration data	Medium	Medium	Medium
Client system configuration data	High	High	Medium
Scripts and other personally written software	Medium	High	Medium
Contact information (address book)	Medium	High	Medium
Research sources and findings	Medium	Medium	Medium
Web bookmarks	Low	Medium	Medium
Legal documents	High	High	Medium
Virtual PC Data	Medium	Medium	Medium
Installed software registration serial numbers and contact information	High	High	Medium
High Water Mark	**High**	**High**	**Medium**

Note on OICM:
The information under consideration for this exercise is not a prime candidate to demonstrate the value received for the effort involved in constructing the OICM due to the relatively small size of the data set. A larger organization with a more diverse and extensive variety of information would accrue much more benefit from the classification of data, the examination of the relative value of the differing data types, and the corresponding analysis of resources expended for information protection for each type. In this instance, the small amount of information under consideration allows for a relatively equal protection focus.

2. Which systems process, store, or transmit the critical information?
System Information Criticality Matrix
For the purpose of this exercise, a System Criticality Matrix would be of extremely limited utility and will not be created, as the client's data resides on a single system and any network access points are not under this organization's control. High water marks for the SCM will be pegged at "Medium" for availability, and "High" for integrity and confidentiality.

3. What are the operational processes involved in the processing, storage and/or transmission of the critical information?

Access to the organization's Internet Service Provider is achieved by means of the OpenSSH[11] capabilities included in OS X. This access method is mandated by the policy of both the organization and the ISP, which disallows unencrypted (telnet) access to the shell account. POP, SMTP, and NNTP traffic is forced to travel through encrypted tunnels generated by OpenSSH. However, as of this writing the ISP only supports the use of SSH protocol version 1, which is subject to known vulnerabilities[12]. This exposure is beyond the reach of the target organization to mitigate, but plans to adopt SSH Protocol Version 2 for this access are in place when the updated protocol becomes available. The risk of compromise is minimized by not initiating unencrypted SSH sessions. The ISP is aware of the exposure, but is bound by other priorities. Due to increased levels of unsolicited email (UCE/"SPAM"), and various forms of malicious code transmitted via email, the organization has adopted a practice of logging in to a LINUX shell account provided by the ISP and examining inbound email while still on the server via the UNIX mail client "mutt"[13]. Suspicious/unsolicited offerings are then deleted before legitimate email is downloaded via a SSH tunnel to the client system. This practice, along with the usage by the ISP of the Open Source utility "SpamAssassin"[14] has served to minimize the effect of UCE and email-borne malware on the target system while assuring confidentiality. Internet banking, and other confidential activities are transacted via the HTTPS protocol as implemented in Apple's "Safari" web browser which supports 128 bit encrypted connections via Open SSL. Data contained in the system is processed by a variety of commercial, freeware, and Open Source applications. The information is stored on the system local hard drive and confidentiality is protected by the use of PGP Corporation's PGPDisk[15]. Data integrity and availability are assured by the practice of conducting regular full and partial backups on an as-needed basis.

A detailed assessment and technical evaluation of the application software used is outside the scope of this investigation.

4. What is the appropriate information security posture for these systems?

This system does not contain information of any value to anyone other than the owner; consequently there is an extremely low likelihood of a specifically targeted

[11] "OpenSSH features"
URL: http://openssh.com/features.html - Port Forwarding

[12] SSH Communications Security
SSH Company News Room
"Secure Shell version 1 vulnerabilities reported by CERT"
URL: http://www.ssh.com/company/newsroom/article/212/

[13] "The Mutt Email Client"
URL: http://www.mutt.org/

[14] Spam Assassin
"Welcome to SpamAssassin"
URL: http://www.spamassassin.org/index.html

[15] PGP Corporation
"PGP Personal Desktop"
URL: http://www.pgp.com/products/personal/features.html

effort by skilled persons to penetrate system security. Protection efforts therefore shift to the area of basic security practice such as promptly applying system updates, system hardening, regular backups, and employing operational procedures of a reasonably secure nature. Extreme protection measures are not cost-effective or indicated for this organization. There are several security measures available with OS X that are designed for use in a multi-user environment such as "Password Server" that are not in use or needed for this single user system.

5. What are the potential system vulnerabilities?
Loss of data integrity or availability due to system malfunction or operator error.

Possibility of vectoring malicious code to other systems due to lack of antivirus scanning capabilities

Poor documentation and system configuration management practices could increase time needed to restore system after catastrophic or partial failure.

System directories are not encrypted and could potentially provide access to sensitive information for unauthorized users.

Temporary loss of data availability due to physically separate storage of system backups

Lack of file integrity software/checksumming of system binaries increases the risk of potential system compromise.

Adequacy of system logging and network traffic controls are in question.

Lack of Intrusion Detection System could increase the possibility of undetected system compromise.

Physical security issues

Loss of system control or compromise of information CIA due to activities of third parties

6. What are the potential solutions to remediate or eliminate the identified vulnerabilities in a cost effective manner?

Loss of data integrity or availability due to system malfunction or operator error
This exposure is remediated by the practice of regular full and partial backups.

Possibility of vectoring malicious code to other systems due to lack of antivirus scanning capabilities
This exposure would be minimized by the purchase of a reliable anti-virus product.

Poor documentation and system configuration management practices could increase time needed to restore system after catastrophic or partial failure

Exposure can be reduced by better documentation of system functions and configuration. Unfortunately, this effort is not a high priority.

System directories are not encrypted and could potentially provide access to sensitive information to unauthorized users

This exposure, while real, is one that has a low probability of exploitation due to low value of information on target system to anyone but the owner.

Temporary loss of data availability due to physically separate storage of system backups

One way to mitigate this exposure is the purchase of additional external hard drives for use as backup media, keeping one with the system, and storing the other offsite. At this time, this practice is not necessary. Potential system downtime while fetching remotely stored backups is an acceptable risk to the organization.

Lack of file integrity software/checksumming of system binaries increases the risk of potential system compromise

Mitigation of this exposure will require purchase and installation of file integrity checking software such as Tripwire[16]. Installation of this software would lead to unacceptable disruption of daily system operation due to the need for a complete reinstallation "from scratch" of the OS X operating system and all applications. A manual examination of system directory listings will provide limited assurance of system integrity. Some form of checksumming software will be installed at some point in the future, probably along with the next major operating system upgrade.

Adequacy of system logging and network traffic controls

Technical evaluation of system logging and network traffic controls is needed and will be included in a subsequent section of this report.

Lack of Intrusion Detection System could increase the possibility of undetected system compromise

Installation of an IDS has not been deemed cost-effective in this particular situation. All externally instigated inbound traffic is blocked by firewall rules. The later technical evaluation of existing traffic controls may indicate a more pressing need for an IDS.

[16] Tripwire Inc.
"Change Monitoring and Reporting Systems"
URL: http://www.tripwire.com/

Physical security issues
Lock it up with cable lock. Watch it closely. User directories are encrypted in case of physical compromise. Open Firmware Password is enabled, which configures the system to require a password in order to boot. This would deny information access in event of system theft

Loss of system control or compromise of information CIA due to activities of third parties
Install network traffic control system (firewalls). Practice password discipline. Harden system. Make sure that available software updates are installed promptly. Perform technical evaluation of system to validate the previous steps.

The results of the examination of each of the 18 baseline information security categories will be presented in Assignment 4.

Preliminary Findings
For the most part, the system is operated in a manner consistent with good practice within the needs and capabilities of the owner. OS hardening steps have been taken. A better firewall configuration than the one included with the standard OS X configuration has been installed. Software updates, when made available, are promptly installed. Proper password discipline is followed. A potential vulnerability uncovered in the course of the assessment is the lack of checksum protection of system executables. Purchase of a suitable OS X anti-virus scanner is also indicated along with the possible need for an Intrusion Detection System. Updating and organizing system documentation is also necessary, but is not a high priority for the system owner. Hopefully, this paper will enhance documentation of this system. Currently used data protection methods are considered effective for this system. Encrypting the user disk directories with PGP Corporation’s "PGPDisk" provides confidentiality of user data. Irregularly scheduled but frequent verified backups protect integrity and availability. In order to alleviate concerns regarding system configuration, and to validate system operational practices, further technical evaluation is indicated in the following area:

Apple OS X V 10.3.3 configuration and usage including
Network Traffic Controls and Logging and Auditing Capabilities
The evaluation plans for these areas are included in Assignment 2, and the actual evaluations and results are included here in Assignment 3.

Modified NSWC Vulnerability and Countermeasure Check List
Evaluation Objectives:
The objective of this evaluation is to provide assurance that the target system is being operated in the most secure manner possible within the constraints of budget and operational necessities. An additional objective is to construct an evaluation checklist that will be of use as a starting point for other evaluations.

Checklist has been modified from original NSWC version to enhance consistency and readability, and to provide a more thorough examination.

Mark each as True, False, or NA - not applicable.
In the absence of indications to the contrary, the Information System is operating at an acceptable risk when all of the leftmost countermeasures are marked 'True'. For all leftmost items not marked as "True", indicate in the section entitled "comments" how the risk is mitigated by other means OR why the vulnerability is at an acceptable level.

NOTE: if any of the compliance entries is FALSE, indicate in the section entitled "comments" how the risk is managed.

ST&E = Security Test and Evaluation**.**

1. Target System
A portable single user endpoint system that is utilized in a variety of circumstances ranging from hotel room dialup or broadband access, public wireless access points, to highly secured installations.

2. Adequacy of Training
Control Objectives:
Verify that personnel are adequately trained to perform assigned duties

Control Description
Determination of adequacy of training is accomplished by interviews and background checks.

Potential Risks:
Inadequately trained persons are a greater threat to information CIA than are persons with malicious intent because there are far more incompetent people in the world than there are actively evil people.

"Never ascribe to malice that which can be explained by incompetence"[17]

Statements of Compliance:
Administrator
(_True_) System administrator has successfully completed vendor provided (or equivalent) training for this Operating System.

[17] Napoleon Bonaparte

Name of System Administrator: Claude V. Lucas
Date and location of training: Ongoing and continuous.
Users
(_NA_) All authorized users have successfully completed Information Security training
(_NA_) Users and administrators have been "cross trained" to perform job functions of other persons.
(_NA_) Users know to contact the IS Security Officer when an incident occurs.
(_NA_) New employees are briefed on computer security responsibilities.
Security Officer
(_True_) ISSO is knowledgeable about the security features and vulnerabilities of this IS.

Verification of training is by examination of training certificates and resumes belonging to operational staff, and by background check if indicated.

Comments: The system owner is the IS Security Officer who is the system administrator who also is the user community…
Continuing technical education is a high priority for this organization.

Risk Rating: (_X_) High (__) Moderate (__) Low
Justification of rating:
Risk rating is high due to high potential of inadequately trained personnel causing loss of data CIA
ST&E: (_X_) Pass (__) Fail

3. Malicious Code Protection - Anti-Virus
Reference:
Al Fasoldt
technofile
"Mac OS X computers don't need antivirus software,
but users should avoid forwarding suspicious mail"
URL: http://aroundcny.com/technofile/texts/mac070203.html

Control Objectives:
Assure that the target system is not vulnerable to the introduction of any type of virus or other malicious code.

Control Description
Anti-virus software should scan newly introduced files for potentially malicious code, attempt to deal with malware according to program design and configuration, and promptly inform the system operator of any triggering events

Potential Risks:
Infection of target system, possibility of vectoring malware to other systems
Possibility of OS X infestation or transmission is low, but greater than zero.

Statements of Compliance:
(_False_) Norton Anti-Virus for Mac OS X or other anti-virus scanning product has been installed on IS.
Frequency of virus scans:________________________________
Frequency of AV signature updates ________________________________
(_N/A_) Virus software signature files and updates are regularly looked for and applied if available.
Automatic Scans or Manual Scans (Circle one)

Verification is by examination of system.
Examine directory structure for installed anti-virus program files.
Examine running processes listing for anti-virus programs in active state.
If installed, open anti-virus console and verify signature update scheme and
automatic scheduling, if implemented.
Note date and time of last signature update
Force a signature update from master signature file.
Verify proper installation of new signature update by system examination.
Introduce an anti-virus test file such as the one available from eicar.org[18] to the
system via email and/or direct copying from media and/or network.
Observe and report results.

Comments
OS X Anti-Virus Software has not, as of yet been determined to be cost-effective for this system due to lack of native OS X virii. If an OS X virus is discovered in the wild then appropriate countermeasures will be promptly implemented. OS X anti virus software should be installed in order to minimize risk of inadvertent transmission of malicious code to vulnerable external systems.
Norton AntiVirus 2002 for Windows is installed in the MS Windows subsystem and appropriately configured to update signatures automatically, but has not been evaluated for this report.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is moderate due to lack of OS X virii and to strong email screening procedures
ST&E: (_X_) Pass (__) Fail

4. Malicious Code Protection - File Checksumming
Reference:
Tripwire Inc.
"Change Monitoring and Reporting Systems"
URL: http://www.tripwire.com/products/index.cfm

[18] Online Eicar
"Anti-Virus test file"
1 May 2003
URL: http://www.eicar.org/anti_virus_test_file.htm

Control Objectives:
Assure that system is not vulnerable to the introduction of altered system files.

Control Description
File integrity checking software protects a system against surreptitiously introduced copies of operating system files with altered functions by creating a mathematical checksum for each file and storing the checksum in a database where it can be retrieved to verify files have not been changed.

Potential Risks:
An attacker could possibly replace system files with altered versions designed to perform additional undesired functions

Statements of Compliance:
(_False_) File integrity software is routinely run to flag modifications to files.
(_False_) Procedures for protection/prevention are incorporated in SOPs (including procedures for evaluating and testing code downloaded from the internet or other sources).
(_False_) All code is evaluated on another standalone system prior to use on this IS.
(_NA_) Suspected and confirmed incidents are reported to the ISSO.

Verification is by demonstration
Examine directory structure for installed program files.
Examine running processes for file integrity programs in running state.
Introduce file with different checksum than expected by integrity checking software. Run validation check and observe results

Comments
System has not had file integrity/checksumming software installed. This oversight needs to be addressed. Checksumming software such as Tripwire is definitely indicated and should be installed as soon as possible. It is not yet determined if this effort will require a complete reinstall of software from known good sources. System reinstallation is a major undertaking, which is an operational consideration for such a project.
Lack of file integrity checking earns a "fail" for this section.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is moderate due to lack of protection but not high due to remote possibility of exploitation.
ST&E: (__) Pass (_X_) Fail

5. Software Maintenance Updates

Reference
Jim Dalrymple
"Mac OS X Software Update Security Issue Uncovered"
MacCentral
July 08, 2002 9:05 pm
URL:
http://maccentral.macworld.com/news/2002/07/08/update/index.php?redirect=1081111615000

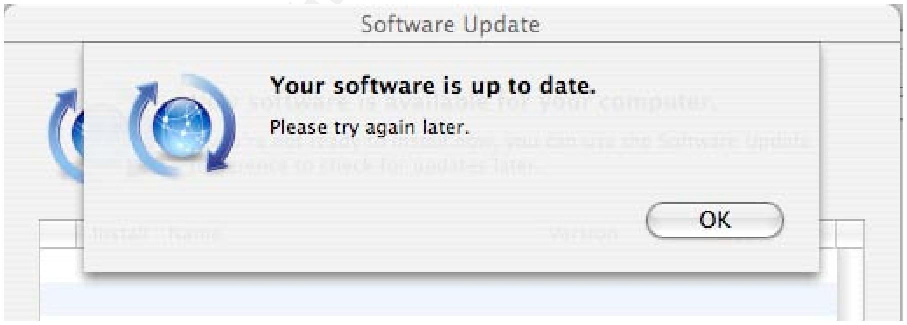
Control Objectives:
Assure that all software maintenance updates are installed in a timely manner.

Control Description
Software Update is an Apple provided utility that keeps track of the versions of installed software. When invoked, it checks for updates via the Internet and informs the operator if new program versions are available. It can be configured to automatically check for updates and install them without operator intervention.

Potential Risks:
Out of date software can contain easily exploited vulnerabilities.
It is theoretically possible for a determined attacker to spoof the Apple software update host's Internet address and cause users to update from the wrong host.

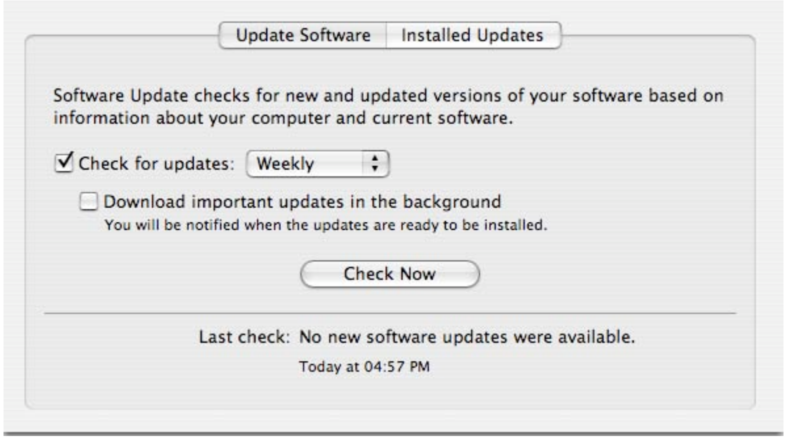
Statements of Compliance:
(_True_) All vendor recommended Security-related patches have been applied.
(_True_) The system administrator updates operating system and application patches at least quarterly.

Verification is by demonstration and observation:
Run "System Update" utility, if all appropriate patches are installed, it will indicate that the system software is up to date. Attach screen shot.



Your software is up to date.

Please try again later.



Software Update checks for new and updated versions of your software based on information about your computer and current software.

☑ Check for updates: Weekly

□ Download important updates in the background
You will be notified when the updates are ready to be installed.

Last check: No new software updates were available.
Today at 04:57 PM

Comments
System software is currently up to date and Software Update is configured to automatically check weekly for new updates.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating of system exposure due to exploitation of yet undiscovered vulnerabilities is low due to timely updates by manufacturer. Risk of update site being hijacked is also low. Both risks, however, are greater than zero.
ST&E: (_X_) Pass (__) Fail

6. Account Management
Reference:
URL: Leon Towns-von Stauber
Occam's Razor Mac OS X Presentations:
“Security”
URL: http://www.occam.com/ocr/osx/

Control Objectives:
Assure that account management is being performed in accordance with policy

Control Description:
No automatic controls are in place.

Potential Risks:
Unneeded or unused accounts provide potential unauthorized access points.

Statements of Compliance:
(_False_) A copy of the written enforced process for establishing, using, and terminating an account for this IS is attached to this risk assessment.
(_True_) All accounts are password protected.
(_True_) Guest / anonymous accounts/access are not allowed except to allow non-interactive function of various system processes.

Verification is by examination of the netinfo database for this system which shows that all accounts other than "root" and that of the system owner have the default shell set to /usr/bin/false or /dev/null.

Comments
Account management is not a significant issue for a single user system.
Other than the root account and the owner's account the only other accounts are to allow non-interactive functioning of various system processes. Non-interactive accounts on this system have been examined and are verified as being necessary for ongoing system operations. Detailed evaluation of security concerns regarding the "netinfo" authentication scheme as implemented in OS X is beyond the scope of this investigation. There is no written account management process to include in this evaluation. Some sources discourage the enabling of the root account, but it is in use on this system.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating is low due to no turnover of accounts
ST&E: (_X_) Pass (__) Fail

7. Password Management
Reference
Leon Towns-von Stauber
Occam's Razor Mac OS X Presentations:
"Security"
URL: http://www.occam.com/ocr/osx/

Control Objectives:
Assure that safe password usage practices are in effect.

Control Description:
No automatic controls are in place. Control is procedural.

Potential Risks:
Easily guessed or computed passwords are a major enabler of unauthorized system access or privilege elevation.

Statements of Compliance:
(_True_) Only the user knows user passwords.
(_True_) Passwords are never stored in clear text (unencrypted).
(_True_) Passwords are at least seven characters in length.
(_False_) Passwords automatically expire at least yearly OR
(_True_) Passwords are changed at least once a year.
(_True_) Users are required to maintain unique passwords for each IS.
(_True_) Password tester (e.g., crack) is run at least yearly.
(_True_) Administrator (root) password is protected to the same level as the data contained on the IS.
(_False_) Apple "Password Server" function is enabled on this system.

(_True_) Root account is enabled on this IS

Verification by interview:
The system owner confirms these statements and configuration choices have been manually verified.
No technical verification has been performed at this time.

Comments
OS X "Password Manager" is not in use on this system. No shadow password file has been created and lookupd is configured to directly access the netinfo database. These configuration choices, while appropriate for a single-user system, do not enable any automatic password controls such as expiration or length controls. Therefore, password discipline is a responsibility of the system owner. Password issues, other than choosing an adequate password and frequently changing it, are not judged to be significant in this instance. The root account is enabled on this system, which is considered by some to be an unnecessary exposure.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is moderate due to lack of password controls.
ST&E: (_X_) Pass (__) Fail

8. Network Daemon Services
Reference:
SANS Advanced System Audit: UNIX Workbook pp 61-73

Control Objectives:
Verify that all services invoked by the UNIX network daemons "inetd" and "xinetd" are enabled for valid business reasons, and that all services not needed for valid business reasons are effectively disabled.

Control Description
Enabling or disabling of network daemon services is a matter of system configuration. Control is a matter of an educated examination of system configuration files and system scanning.

Potential Risks:
Inappropriately enabled network services present many risks to secure system operations including, but not limited to possibility of unauthorized access and unauthorized elevation of privilege

Statements of Compliance:
(_False_) TCP Wrappers or equivalent are run.
(_False_) All inetd TCP Services have TCPwrappers with access control lists.
(_False_) The access control files deny all services to all computers and then permit access only to hosts that require access, and only to necessary services.

Verification is by manual review of configuration files and process listings.
Technical verification is provided by nmap and nessus scans.

Attach a printed copy of the following files: Network daemon configuration file (ex. inetd.conf, xinetd.d files)
Relevant files are included in Appendix 1

Comments
All network daemon services are invoked from xinetd rather than inetd.
All services in /etc/inetd.conf are disabled by being commented out.
The only network daemon invoked service enabled on the system is Qualcomm's POP utility "qpopper" operating on port 110. Access to this utility is limited to the local system and is not available to external systems. This restriction is enforced both by the firewall blocking the inbound port with the default deny rule, and the configuration file /etc/xinetd.d/qpopper allowing access only from localhost. TCPwrappers is included in OS X, but due to these restrictions, the use of TCPwrappers is not considered necessary.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Low risk due to low number (1) of services provided and access restrictions
ST&E: (_X_) Pass (__) Fail

9. Unneeded Services
References:
SANS Advanced System Audit: UNIX Workbook pp 61-73, system "man" pages, and
Gordon Davisson
"Mac OS X: What Are All Those Processes?
A short list of background processes and daemons"
Westwind Computing
URL: http://www.westwind.com/reference/OS-X/background-processes.html

Control Objectives:
Verify that all services available from this system are activated for a valid business reason. Verify that no unneeded services are provided.

Control Description
Enabling or disabling of system services is a matter of system configuration. Control is a matter of an educated examination of system configuration.

Potential Risks:
Unneeded services consume system resources and are a source of potential vulnerabilities.

Statements of Compliance:
(_True_) Unneeded services are disabled.

Verification by demonstration:
Identify and describe active processes.
Run "ps axuc" in shell window
Include output in report
Detailed process listing included in Appendix 2

Identify and describe all listed processes

init
primal UNIX process
mach_init
Mach service naming (bootstrap) daemon.
syslogd
System logger
kextd
daemon process that loads kernel extension on demand
configd
configures and maintains the network
diskarbitrationd
notifies clients of the appearance of disks and filesystems
notifyd
handle notify messages
netinfod
NetInfo servers, one for each domain served.
update
daemon that flushes internal file system caches to disk
dynamic_pager
Virtual memory handler
coreservicesd
handles drag and dropping
distnoted
distributed notification server
mDNSResponder
multicast-DNS responder, which supports Rendezvous, Apple's implementation of zero-configuration networking
KernelEventAgent
handles one of the core system services (events such as file systems being mounted and unmounted, low disk space, network connections going down, etc.)
cron
Executes scheduled commands or scripts

SecurityServer
oversees system authorization, authentication, and keychain access
WindowServer
Window Server process
ATSServer
Apple Type Services daemon

loginwindow
login front end for the console of the Mac OS X environment

ntpd
Network Time Protocol

DirectoryService
part of the MacOS X information and authentication subsystem

lookupd
directory information and cache daemon

crashreporterd
crash logger

cupsd
The CUPS printing services daemon. This daemon schedules printing tasks.

xinetd
listens for connections on certain sockets. When a connection occurs, it decides what service the socket corresponds to and invokes the appropriate program to service the request

httpd
webserver process

master
part of postfix Mail Transport Agent

pbs
enables the exchange of data between applications

Dock
Part of GUI

SystemUIServer
controls the menu extras and fast user switching,

Finder
File system browser

LittleSnitchDaemon
Outbound traffic controller

PGPdiskEngine
Virtual disk decrypt/encrypt

Terminal
Shell window handler

login
login process handler

Safari
web browser

qmgr
part of postfix Mail Transport Agent

ssh
secure external communications

Microsoft Word
word processor

Microsoft Database Daemon
MS Office database

SecurityAgent
manages the user authentication process.
ps
process listing utility

Verify that all active processes are needed and present no vulnerabilities.
All running processes are performing needed functions. Vulnerability assessment of OS X system processes and installed applications is beyond the scope of this exercise. All appropriate system and application updates have been applied.

Run "netstat -a" in shell window
Include output in report
Active Internet connections (including servers) and Active LOCAL (UNIX) domain sockets listing included in Appendix 3
Identify and describe all listed services

Active Internet connections (including servers)
Local Address
localhost.10025
Local endpoint of SSH tunnel to SMTP server

localhost.10110
Local endpoint of SSH tunnel to POP server

x.x.x.x.49398
Outbound SSH

localhost.ipp
**.ipp*
Internet Printing Protocol

**.pop3*
Email server process

**.http*
**.https*
WebServer

localhost.netinfo-local
localhost.954
network information process

**.rockwell-csp2*
**.3942*
Microsoft Database Daemon

**.mdns*
Multicast DNS

z.z.z.z.ntp
localhost.ntp
**.ntp*
Time Services

**.bootpc*
DHCP Service

**.syslog*
**.514*
System logging facility

Active LOCAL (UNIX) domain sockets

/tmp/.pgpdisk-claudel-501-sock
Data Encryption Program
private/bsmtp
used by postfix Mail Transport Agent
private/ifmail
used by postfix Mail Transport Agent
private/uucp
used by postfix Mail Transport Agent
private/cyrus
used by postfix Mail Transport Agent
private/old-cyrus
used by postfix Mail Transport Agent
private/maildrop
used by postfix Mail Transport Agent
private/lmtp
used by postfix Mail Transport Agent
private/virtual
used by postfix Mail Transport Agent
private/local
used by postfix Mail Transport Agent
private/error
used by postfix Mail Transport Agent
public/showq
used by postfix Mail Transport Agent
private/relay
used by postfix Mail Transport Agent
private/smtp
used by postfix Mail Transport Agent
private/proxymap
used by postfix Mail Transport Agent

public/flush
used by postfix Mail Transport Agent

private/defer
used by postfix Mail Transport Agent
private/bounce
used by postfix Mail Transport Agent
private/rewrite
used by postfix Mail Transport Agent
public/cleanup
used by postfix Mail Transport Agent
/var/run/pppconfd
PPP configuration daemon
/var/run/mDNSResponder
MulticastDNS client
/var/run/syslog
System logging process

Verify that all active services are needed and present no vulnerabilities.
Operational necessity of services verified by interview with system owner
Detailed vulnerability assessment of system services is beyond the scope of this evaluation.

Run "lsof -i" in shell window
Include output in report

```
COMMAND    PID   USER   FD   TYPE   DEVICE       NODE NAME
ssh        638  claudel  3u  IPv4  0x02a70570    TCP  x.x.x.x:49398-> isp.net:ssh (ESTABLISHED)
ssh        638  claudel  4u  IPv6  0x02a83e80    TCP  localhost:10110 (ESTABLISHED)
ssh        638  claudel  5u  IPv4  0x02a70824    TCP  localhost:10110 (LISTEN)
ssh        638  claudel  6u  IPv6  0x02a83cd0    TCP  localhost:10025 (LISTEN)
ssh        638  claudel  7u  IPv4  0x02a702bc    TCP  localhost:10025 (LISTEN)
Microsoft  814  claudel 15u  IPv4  0x033dafd0    TCP  *:3942 (LISTEN)
Microsoft  814  claudel 24u  IPv4  0x01d89700    UDP  *:rockwell-csp2d8970 UDP
                                                          *:rockwell-csp2
```

Identify and describe usage of all listed ports
Ports 49398,10110 and 10025 are in use by SSH <> to the ISP, with 10110 and 10025 corresponding to the client endpoints of the POP and SMTP tunnels. The remaining ports are in use by the Microsoft Database Daemon while components of Microsoft Office X are operational.

Comments
All running services, open sockets, and open ports are in use by valid system processes. Vulnerability assessment of applications is beyond the scope of this exercise.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is moderate due to number of services and processes in use
ST&E: (_X_) Pass (__) Fail

10. Regularly Scheduled Tasks

References:
system man pages for "cron" and "periodic"

Control Objectives:
Verify the valid need for any automatically executed programs

Control Description:
Manually examine /etc/crontab and the /etc/periodic directories. Verify each automatically executed program is performing needed functions.

Potential Risks:
Unauthorized cron jobs present potential threats to information CIA

Statements of Compliance:
(_False_) The facility to automatically execute periodic tasks on this computer (cron) has been disabled on this computer
(_False_) There are no automatically executed periodic tasks running on this computer.

Verification:
Either verify cron is disabled, or include /etc/crontab and listing of /etc/periodic/* in report.
Verify all cron jobs are performing valid tasks

```
#cat /etc/crontab

# /etc/crontab
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin
HOME=/var/log
#
#minute hour    mday    month   wday    who     command
#
*/5     *       *       *       *       root    /usr/libexec/atrun
#
# Run daily/weekly/monthly jobs.
10      *       *       *       *       root    /sw/sbin/anacron -s
58      *       *       *       *       root    /usr/sbin/ntpdate -bvs > /dev/null 2>&1
```

Comments
/usr/libexec/atrun (from system man page)
Atrun runs jobs queued by at(1). Root's crontab(5) must contain the line:

```
*/10    *       *       *       *       root    /usr/libexec/atrun
```

so that atrun(8) gets called every ten minutes.

/sw/sbin/anacron -s (from man page)

Anacron can be used to execute commands periodically, with a frequency specified in days. Unlike cron(8), it does not assume that the machine is running continuously. Hence, it can be used on machines that aren't running 24 hours a day, to control daily, weekly, and monthly jobs that *are usually controlled by cron.*

Anacron[19] helps cron "catch up" when a system is shut down. This is essential for a laptop system that can be turned off for extended periods.

/usr/sbin/ntpdate -bvs > /dev/null 2>&1
Updates system time from network time server

Examine contents of the /etc/periodic directory tree in report.
Verify all periodic tasks are needed and are being performed for valid reasons.

/etc/periodic/daily:
100.logcheck
    Creates "logcheck" reports
400.clean-logs
    recycles system logs
500.daily
    performs housekeeping functions

/etc/periodic/weekly:
500.weekly
    performs housekeeping functions

/etc/periodic/monthly:
500.monthly
    performs housekeeping functions

Comments:
Assessor has examined the periodic files and verifies that all tasks are needed for valid system purposes. File listings are not included in this report due to space considerations.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating low due to low probability of compromise
ST&E: (_X_) Pass (__) Fail

11. Network and Remote Access
Control Objectives:
Verify the existence of all network and remote access devices in this system.

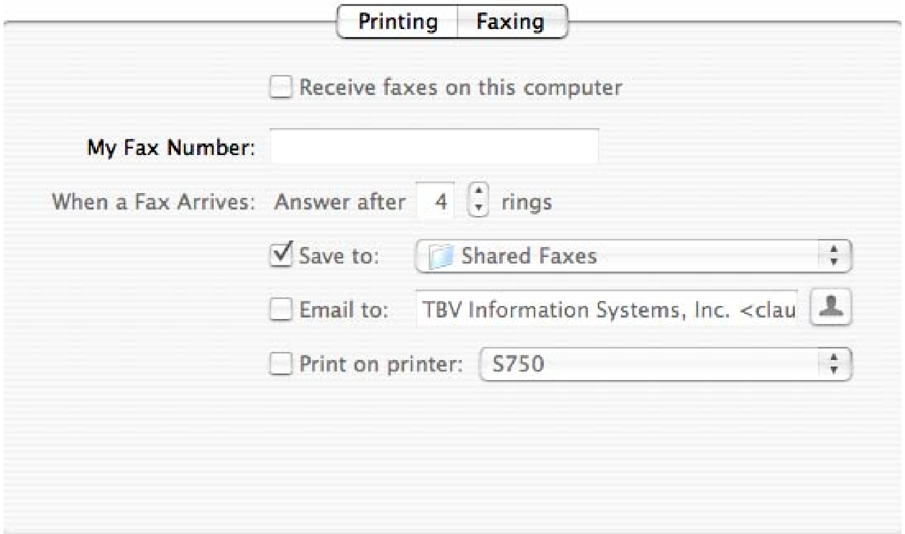
Control Description:
Control is manual examination of system configuration

[19] "What is Anacron?"
URL: http://anacron.sourceforge.net/

Potential Risks:
Network and remote access devices potentially allow unauthorized access.

Statements of Compliance:
(_False_) There are no modems connected to this computer.
(_True_) All modems connected to the system have "auto-answer" disabled or are attached to phone lines that restrict incoming calls.
(_False_) This computer has only one network connection (no dual interfaces).

Verification of hardware configuration is accomplished by examination of the listing provided by the included utility "System Profiler.
Verify auto-answer is disabled in modem configuration by accessing fax control panel in the System Preferences utility and attaching screen shot.



☐ Receive faxes on this computer

My Fax Number:

When a Fax Arrives: Answer after 4 rings

☑ Save to: Shared Faxes

☐ Email to: TBV Information Systems, Inc. <clau

☐ Print on printer: S750

Comments
Internal modem, External cellphone modem, built in 802.11 wireless, and ethernet interface are installed, but are all subject to the same usage policies. Modem is configured to not answer incoming calls, and generally is not connected to a phone line unless it is in use.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating is low due to infrequent use
ST&E: (_X_) Pass (__) Fail

12. Data Exports
Reference:
SANS Advanced System Audit: UNIX Workbook pp 93-97

Control Objectives:
Assure that unauthorized information disclosure does not occur via use of Network File System, SAMBA, or other means utilizing Remote Procedure Calls.

Control Description:
Control is accomplished by manual examination of system configuration and program listings and by scanning.

Potential Risks:
Compromise of information CIA via exploitation of data export services.

Statements of Compliance:
NFS/RPC
(_True_) System does not export information via Network File System.
(_True_) System does not export information via SAMBA.
(_False_) System has a known secured portmapper (securelib, SunOS with patch id 100482-02 or later, Irix 4.0.x)and has access lists in place. OR
(_False_) Portmapper is protected by portmapper/rpcbind replacement that uses TCP Wrappers access list - depending on OS it's called either portmapper or rpcbind
(_True_) Portmapper is not running.

Verification by observation of system:
Examination of the listing of running processes generated earlier shows the absence of running NFS processes, either client or server. This listing also indicates the absence of a running portmapper. This examination is confirmed by nessus scan.

Comments
Portmapper, NFS and SAMBA are disabled on this system.
No data exports are enabled.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating is low due to data export services being disabled
ST&E: (_X_) Pass (__) Fail

13. Information disclosure via obsolete UNIX utilities
Reference:
Carnegie-Mellon University Software Engineering Group
CERT Coordination Center
“UNIX Security Checklist v2.0
2.0 Network Services”
URL: http://www.cert.org/tech_tips/usc20_full.html - 2.0

Control Objectives
Verify that unsafe legacy applications do not enable vulnerabilities.

Control Description
Control is accomplished by manual examination of system configuration and program listings, and by scanning.

Potential Risks
Unauthorized system access, elevation of privilege, data compromise. due to poor authentication in older UNIX system utility programs.

Statements of Compliance:
(_True_) IS does not allow anonymous access (ftp, telnet, etc).
(_True_) IS does not allow r utilities (rlogin / rshell / rexec) from addresses external to the site.
(_True_) IS does not allow information queries (e.g. World Wide Web (HTTP) or similar (archie, gopher, etc.)) from addresses external to the site.
(_True_) IS does not provide mail service (mail reflector, POP, etc.) to locations (addresses) external to the site.
(_True_) IS does not provide information, by any other method to unauthenticated users, programs etc. to locations (addresses) external to the site.

Verification
Statements from this section are verified by examining the results of a nessus scan, and by examining the network daemon configuration files /etc/inetd.conf, the files in /etc/xinetd.d and the ipfw ruleset in /etc/ipfw.conf. nessus scan results and the indicated configuration files are included in the appendices.

Comments
Indicated services are disabled and/or access is denied from external systems.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating is low due to services being disabled
ST&E: (_X_) Pass (__) Fail

14. Misuse of Resources Warnings
Reference:
System man page for "motd"

Control Objectives:
Verify appropriate banner warnings are presented to potential system users before logon is allowed.

Control Description:
Control is accomplished by manual examination of system configuration

Potential Risks:
Intruders can be encouraged by "welcome" banners.

Statements of Compliance:
(_False_) Login banner containing an abbreviated version of the organizational acceptable use policy is displayed at logon for each user.

(_False_) Login banner advises users that use is subject to monitoring and that use constitutes consent to monitoring.

Verification by examination of file /etc/motd

Comments
Interactive logins are allowed only at the "console" of the PowerBook. No warnings or acknowledgement of connection are displayed for remote access attempts.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Low risk due to "no connections allowed" policy
ST&E: (_X_) Pass (__) Fail

15. Media Marking
References: NA

Control Objectives:
Verify all removable media is appropriately labeled.

Control Description:
Policy issue. No automatic controls are in use.

Potential Risks:
None, in this situation

Statements of Compliance:

(_NA_) All magnetic media containing data protected by the "Privacy Act of 1974" is marked "Privacy Act".
(_NA_) All hardcopy reports containing Privacy data are marked accordingly when printed.
(_NA_) All "For Official Use Only" (FOUO) data and information is marked as such.
(_NA_) All IS users have been trained to identify Sensitive Unclassified data and properly mark it.
(_True_) All media containing proprietary software is marked to indicate that it is protected by copyright laws.
(_NA_) Sensitive Unclassified/FOUO/proprietary materials are secured when not in use.
(_False_) Burning, shredding, or other method of destruction that will preclude reconstruction of the information disposes of sensitive unclassified hardcopy.
(_True_) Sensitive Unclassified media is overwritten, degaussed, or destroyed by other authorized destruction method.

Verification by interview of system operator

Comments
Obsolete CDs are physically destroyed manually before disposal. No classified or commercially valuable information is processed or stored on this system.
No printouts of interesting information are generated. Purchase of a shredder capable of destroying CDs as well as paper is indicated.

Risk Rating: (__) High (__) Moderate (_X_) Low
Justification of rating:
Risk rating is low due to lack of value of data and adequate procedures
ST&E: (_X_) Pass (__) Fail

16. Open Firmware Password Software
Reference:
CodeSamurai of SecureMac.com
"Open Firmware Password Protection"
SecureMac.com
URL: http://www.securemac.com/openfirmwarepasswordprotection.php

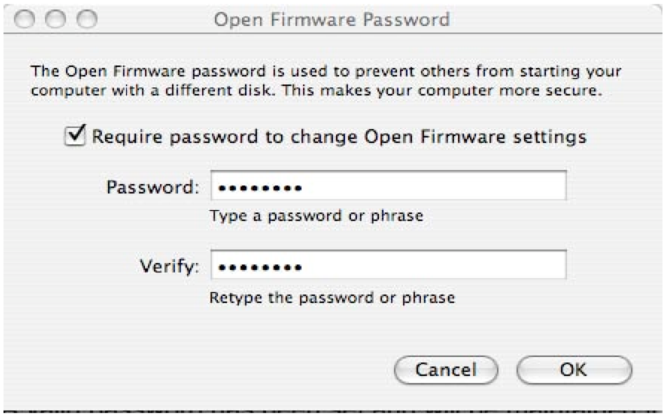
Control Objectives:
Verify the use of the OS X Open Firmware password software to install a password in the system BIOS that restricts ability of system to boot into "single user" mode or on alternate devices.

Control Description:
Apple provided software "Open Firmware Password" allows the system operator to set a password that controls availability of alternate boot possibilities such as "single user" mode or devices other than the system hard drive.

Potential Risks:
Risk of unauthorized persons booting system into "single user" mode or on alternate media and changing/bypassing access controls.

Statements of Compliance:
(_True_) Open Firmware Password software has been installed.
(_True_) A valid password has been set and will be maintained .
(_True_) The software has been configured to prevent unauthorized changing of the boot volume.
(_True_) The software has been configured to prevent unauthorized booting from CD.

Verification
Run Open Firmware Password program.
Attach screenshots



The Open Firmware password is used to prevent others from starting your computer with a different disk. This makes your computer more secure.

☑ Require password to change Open Firmware settings

Password: ••••••••
Type a password or phrase

Verify: ••••••••
Retype the password or phrase

Reboot system, attempt to enter "single user" mode by pressing "Command s" keys after system chime. Attempt to boot from alternate media by restarting system and pressing "Command c" after system chime.

Comments
Open Firmware Password is appropriately configured and denies alternative booting.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is low due to efficacy of operational procedures
ST&E: (_X_) Pass (__) Fail

17. Network Traffic Control

References:
Apple OS X includes an implementation of the traditional UNIX packet filter "ipfw" which is described in the system man pages and by
Chris Cochella
"Configuring Jaguar's Firewall"
O' Reilly MacDevCenter.com
12/27/2002
URL: http://www.macdevcenter.com/pub/a/mac/2002/12/27/macosx_firewall.html

Firewall operations and evaluation procedures are described in the workbook from the SANS Institute Track 7 "Auditing the Perimeter", "Network Auditing Essentials", and by
Craig Robertson in the GCFW certification practical
"Securing GIAC Enterprises: FreeBSD as a Firewall Platform"
January 6, 2003
URL: http://www.giac.org/practical/GCFW/Craig_Robertson_GCFW.pdf

Control Objectives:
Verify that the system network traffic control subsystem is correctly installed, appropriately configured for the organizational mission, and is functioning as expected. Verify that network traffic is being filtered as expected and that notable events are logged to appropriate logfiles

Control Description:
Purpose of the network traffic control subsystem is to regulate inbound and outbound Internet traffic in accordance with policy, which states that all externally invoked inbound communication attempts will be rejected and logged, and certain specific outbound communication attempts will be permitted. The system owner has decided to construct a ruleset controlling the behavior of the OS X ipfw packet filtering function rather than rely on the Apple provided firewall control panel or a shareware utility. This provides a higher degree of control over the firewall capabilities than the available GUI based utilities. Firewall rules will be put in place to mitigate common vulnerabilities such as IP spoofing, source routing, and smurfing. MS Windows networking traffic on ports 137-139 and 445 is of no value or interest and will be silently dropped, as will other common net chatter. All inbound and outbound Internet traffic not specifically allowed is disallowed. This system is an endpoint system, rather than a traffic control device, so the firewall will be evaluated as such. The fact that system policy decrees that no externally initiated inbound traffic is allowed will allow a thorough evaluation by means of scanning.

The following traffic is allowed in normal system operation:

Outbound SSH, WHOIS, DNS, NTP, CVS, HTTP/HTTPS and selected ICMP under stateful inspection.

A regularly used SSH connection to the organization's ISP shell server is configured to bypass check-state inspection in order to enhance network throughput.

Dropped traffic, with the exception of MS Windows networking chatter, is logged to /var/log/system.log via the internal syslog facility.

Control Description
The built in stateful packet filter "ipfw" and the outbound traffic monitor and regulator "Little Snitch" are the mechanisms in place to enforce this policy. "Little Snitch" and "ipfw" are configured to automatically start at system boot time.

Potential Risks:
Risk of loss of data CIA due to unauthorized access to system.

Statements of Compliance:
Firewall Configuration
(_False_) The built-in firewall has been configured to match the /etc/hosts.deny and /etc/hosts.allow files.

(_True_) The built-in firewall has been configured to not respond to malformed or inappropriate TCP/IP 'queries'.

17a. Firewall assessment

What information is the firewall supposed to protect?
What risks are acceptable?
What change control is in effect?

This firewall is configured as an end-point system protection device and as such only regulates traffic to this machine. As no packet filter is considered to be 100% effective, there is a greater than zero risk that a determined attacker could somehow craft a breach. However, this writer is not currently aware of any techniques that would accomplish this action on this particular packet filter. There is no formal change control policy for modifying firewall rules or configuration.

Describe and examine use of ipfw rules from /etc/ipfw.conf.
Static or Stateful rules?

```
cat /etc/ipfw.conf
#ipfw configuration file
#
# Flush all rules
flush
```

Reset firewall at start

```
# Anything in the state table.
add check-state
```

Allows return from internally invoked traffic. This is more secure than allowing established sessions, which can be spoofed.

```
# silent drop Windows/DCE chatter
add deny tcp from any to any 135 in
add deny tcp from any to any 137-139 in
add deny udp from any to any 137-139 in
add deny tcp from any to any 445 in
```

MS Windows networking traffic and DCE traffic is both unnecessary and benign, but bloats the logfiles with useless information.

```
# Allow loopback traffic
add allow ip from any to any via lo0
```

Necessary for normal operation, allows loopback operation

```
# Drop all traffic to 127/8 that doesn't use lo0
add deny log ip from any to 127.0.0.0/8
```

Necessary for normal operation, allows localhost access

```
# Drop fragments
add deny log all from any to any frag in
```

Fragmented packets are dropped and logged
Verified by nessus scan.
Log entry:

```
Mar 28 10:37:34 Blossom kernel: .28 x.x.x.x in via en0 (frag 30416:1144@2960)
```

```
# Reject source-routed packets
add unreach host log ip from any to any ipoptions ssrr,lsrr
```

Source-routed packets are dropped and logged
Verified by nessus scan.
Log entry:

```
Mar 28 10:34:04 Blossom kernel: attempted source route from y.y.y.y to x.x.x.x
```

```
# dhcp / bootps
add allow udp from any 67-68 to any 67-68
```

DHCP service is necessary for mobile operation.

```
#  Allow multicast DNS in
# This rule needs to precede the Drop RFC 1918 rule
add allow udp from any 5353 to 224.0.0.251/8 5353 in
```

OS X uses multicast DNS on 5353 as part of Rendezvous naming scheme
if DNS service is on RFC 1918 net, it would be dropped if this rule was later in the sequence.

```
# Drop RFC1918 addresses on the outside interface
# These rules may cause problems if host is on one of these nets
#add deny log ip from 192.168.0.0/16 to any in
add deny log ip from 172.16.0.0/12 to any in
add deny log ip from 10.0.0.0/8 to any in
#add deny log ip from any to 192.168.0.0/16 in
add deny log ip from any to 172.16.0.0/12 in
add deny log ip from any to 10.0.0.0/8 in
```

```
# Allow SSH traffic <> ISP without state inspection or logging
add allow tcp from any to <isp.net> 22 out
add allow tcp from <isp.net 22> to any in
```

This rule allows frequently used connection to bypass check state for efficiency

```
# Drop any established tcp packets that failed the check-state test.
add deny log tcp from any to any in established
```

Packets claiming to be part of established connections are attempting a spoof

```
# ICMP: (inbound and outbound)
# icmp type 0 = Echo Reply
# icmp type 3 = destination unreachable
# icmp type 4 = Source Quench
# icmp type 8 = Echo
# icmp type 11 = Time Exceeded
# icmp type 12 = Parameter Problem
# icmp type 30 = Traceroute
add allow icmp from any to any icmptypes 0,3,4,8,11,12,30
```

ICMP could present vulnerabilities, but is allowed

```
# SSH (outbound)
add allow tcp from any to any 22 out keep-state
```

Outbound SSH to any destination is allowed

```
# Whois (outbound)
add allow tcp from any to any 43 out keep-state
```

Outbound whois to any destination is allowed

```
# DNS
add allow udp from any to any 53 out keep-state
add allow udp from any to any 5353 out keep-state
add allow tcp from any to any 53 out setup keep-state
```

Outbound DNS queries to any destination are allowed

```
# NTP
add allow udp from any to any ntp out keep-state
```

Outbound NTP client queries to any destination are allowed

```
# CVS
add allow tcp from any to any cvspserver out keep-state
```

Outbound CVS to any destination is allowed

```
# HTTP, HTTPS
add allow tcp from any to any 80 out keep-state
add allow tcp from any to any 443 out keep-state
```

Outbound WWW traffic to any destination is allowed

```
# Drop and log the rest
add deny log all from any to any
```

Deny and log what is not explicitly permitted

Verify /etc/ipfw rules are actually installed:

```
ipfw -a list
00100    0      0 check-state
00200   15    720 deny tcp from any to any 135 in
00300    0      0 deny tcp from any to any 137-139 in
00400    0      0 deny udp from any to any 137-139 in
00500    2     96 deny tcp from any to any 445 in
00600 5124 379512 allow ip from any to any via lo0
00700    0      0 deny log logamount 100000 ip from any to 127.0.0.0/8
00800    0      0 deny log logamount 100000 ip from any to any in frag
00900    0      0 unreach host log logamount 100000 ip from any to any ipopt ssrr,lsrr
01000    0      0 allow udp from any 67-68 to any 67-68
01100    0      0 allow udp from any 5353 to 224.0.0.0/8 5353 in
01200    0      0 deny log logamount 100000 ip from 172.16.0.0/12 to any in
01300    0      0 deny log logamount 100000 ip from 10.0.0.0/8 to any in
01400    0      0 deny log logamount 100000 ip from any to 172.16.0.0/12 in
01500    0      0 deny log logamount 100000 ip from any to 10.0.0.0/8 in
01600  489  29208 allow tcp from any to <isp.net> 22 out
01700  537 115064 allow tcp from <isp.net> 22 to any in
01800    0      0 deny log logamount 100000 tcp from any to any in established
01900    0      0 allow icmp from any to any icmptype 0,3,4,8,11,12,30
02000    0      0 allow tcp from any to any 22 keep-state out
02100    0      0 allow tcp from any to any 43 keep-state out
02200    8   1088 allow udp from any to any 53 keep-state out
02300    0      0 allow udp from any to any 5353 keep-state out
02400    0      0 allow tcp from any to any 53 keep-state out setup
02500    8    608 allow udp from any to any 123 keep-state out
02600    0      0 allow tcp from any to any 2401 keep-state out
02700    0      0 allow tcp from any to any 80 keep-state out
02800    0      0 allow tcp from any to any 443 keep-state out
02900    5    677 deny log logamount 100000 ip from any to any
65535 5296 340244 allow ip from any to any
```

Firewall Policy Assessment.

Firewall policy has evolved to permit traffic that is necessary for day-to-day operation while being as restrictive as is practical.

17b. Firewall technical evaluation

Map open ports with nmap

Analyze results of nmap scans including the following.
Describe exposed services and other interesting results

Internal scans reveal the following services:
TCP connect() scan, SYN scan and SYN scan from port 53 had similar results

```
Strange error from connect (22):Invalid argument
Adding open port 80/tcp
Adding open port 110/tcp
Adding open port 3869/tcp
The 65532 ports scanned but not shown below are in state: closed)

PORT     STATE    SERVICE
80/tcp   open  http
110/tcp  open     pop3
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
3869/tcp open     unknown
Device type: general purpose
Running: Apple Mac OS X 10.3.X
OS details: Apple Mac OX X 10.3.0 - 10.3.2 (Panther)
OS Fingerprint:
```

Exposed services and other interesting results

```
3869/tcp open     unknown
#netstat -a | grep 3869
tcp4       0      0  *.3869                 *.*                    LISTEN
#lsof | grep 3869
Microsoft 372 claudel   15u  IPv4 0x02a3cfd0        0t0      TCP *:3869 (LISTEN)
#ps ax | grep 372
  372  ??  R     12:17.91 /Applications/Microsoft Office X/Microsoft Word
```

TCP port 3869 is in use by MS Word

Port 22 was open by the SSH client during the scan and generated the following error: Strange error from connect (22):Invalid argument

OS Version is actually 10.3.3, but OS update is more recent than the latest nmap

```
Initiating UDP Scan against x.x.x.x at 00:38
The UDP Scan took 433 seconds to scan 65535 ports.
Adding open port 514/udp
Adding open port 138/udp
Adding open port 139/udp
Adding open port 5353/udp
Adding open port 68/udp
Adding open port 137/udp
Adding open port 2222/udp
Interesting ports on x.x.x.x:
(The 65528 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
68/udp   open  dhcpclient
137/udp  open  netbios-ns
138/udp  open  netbios-dgm
139/udp  open  netbios-ssn
514/udp  open  syslog
2222/udp open  unknown
5353/udp open  unknown
Too many fingerprints match this host to give specific OS details
```

Exposed services and other interesting results

```
2222/udp open  unknown
#grep 2222 /etc/services
rockwell-csp2   2222/udp    # Rockwell CSP2
#lsof | grep rockwell-csp2
Microsoft 372 claudel   21u  IPv4 0x01d787d0        0t0      UDP *:rockwell-csp2
#ps ax | grep 372
  372  ??  R     24:29.24 /Applications/Microsoft Office X/Microsoft Word
```

UDP Port 2222 is used by Microsoft Office

UDP Port 5353 is used by multicast DNS

OS fingerprinting unsuccessful

External scan with firewall disabled revealed the following
TCP connect() scan, SYN scan and SYN scan from port 53 had similar results

```
80/tcp    open     http
110/tcp   open     pop-3
```

all other ports visible but "filtered"
OS fingerprinting failed

UDP scan reported

```
68/udp  open  dhcpclient
514/udp open  syslog
Too many fingerprints match this host to give specific OS details
```

External scan with firewall enabled revealed the following:

TCP connect() scan, SYN scan and SYN scan from port 53 had similar results
All 1657 scanned ports on x.x.x.x are: filtered
Too many fingerprints match this host to give specific OS details

UDP scan reported
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1478 scanned ports on x.x.x.x are: filtered
Too many fingerprints match this host to give specific OS details
Ports reported as filtered were listed individually as "open"
This is due to the "ICMP unreachable" method of UDP scanning used by nmap[20] combined with the fact that type 3 ICMP is allowed to pass the firewall

Comments
All ports indicated as "open" by nmap are open for valid reasons, with the exception of the MS windows netbios ports TCP/UDP 137-139. A search for the source of the 137-139 openings with "netstat" and "lsof" produced no results, leading to the conclusion that the nmap finding is a "false positive". In any case, this traffic is denied by firewall rules. The lack of findings of the external scans with the firewall enabled validates the efficacy of the firewall itself.

Scan system with nessus vulnerability scanner

Nessus will be configured to perform all available tests and will be configured to scan the default range (nmap services + privileged ports) of ports using TCP connect().

Perform the nessus scans listed in the evaluation plan.
Save scan results as ASCII text; include nessus reports

Complete nessus scan reports included in Appendix 4
A log of the plugin tests performed by nessus for this section was generated in /usr/local/etc/nessus/nessus.messages, but is not included in the report because of space considerations

Analyze results of nessus scans including any observed event logging.

Describe exposed services and other interesting results

[20] Fyodor <fyodor@insecure.org>
"The Art of Port Scanning"
Insecure.org
(Last significant update: Sat Sep 6 03:24:53 GMT 1997)
URL: http://www.insecure.org/nmap/nmap_doc.html - port_unreach

Internal scan

```
 List of open ports :
   o pop3 (110/tcp) (Security notes found)
   o nessus (1241/tcp) (Security warnings found)
   o unknown (3869/tcp)
   o X11 (6000/tcp) (Security warnings found)
   o bootpc (68/udp)
   o netbios-ns (137/udp)
   o netbios-dgm (138/udp)
   o netbios-ssn (139/udp)
   o syslog (514/udp)
   o general/tcp (Security notes found)
```

Internal scan with firewall disabled for comparison

```
 List of open ports :
   o http (80/tcp) (Security notes found)
   o pop3 (110/tcp) (Security notes found)
   o nessus (1241/tcp) (Security warnings found)
   o unknown (3869/tcp)
   o X11 (6000/tcp) (Security warnings found)
   o bootpc (68/udp)
   o syslog (514/udp)
```

Scan from external machine

```
 List of open ports :
   o general/tcp (Security notes found)

 . Information found on port general/tcp
    The remote host is up
 . Information found on port general/tcp
    HTTP NIDS evasion functions are enabled.
    You may get some false negative results
```

**Scan from external machine with firewall disabled for comparison,
and to simulate firewall breakdown or penetration.**

```
 List of open ports :
   o general/tcp (Security notes found)
   o bootpc (68/udp)
   o http (80/tcp) (Security warnings found)
   o pop3 (110/tcp) (Security notes found)
   o syslog (514/udp)
   o general/udp (Security notes found)

 . Information found on port general/tcp
    The remote host is up
 . Information found on port general/tcp
    HTTP NIDS evasion functions are enabled.
    You may get some false negative results
```

Compare and contrast differing results from nmap and nessus scans.
The nessus internal scan produced the same false positive for the netbios ports as did the previous nmap scan, which is not surprising, as nessus uses nmap to perform port scanning. The only network daemon invoked service enabled on the system is Qualcomm's POP utility "qpopper" operating on port 110. Access to this utility is limited to the local system and is not available to external systems. An apache webserver is serving port 80. Access to the webserver is restricted to localhost in the httpd configuration file and is not allowed from external systems by firewall default deny rule. MS Office X uses the open ports 2222 and 3869. nessus (1241/tcp) has an open port, but this port is in use only while nessusd is running. X11 (6000/tcp) is open during the test for nessus operation. X11 is only used during the operation of X11 based applications. bootpc (68/udp) port is allowed to accommodate DHCP. syslog (514/udp) is in use on the system. Inbound access to nessus, X11, bootpc/DHCP, and syslog service is not allowed from external systems. Multicast Domain Name Service mdns (5353/udp) requires external access to perform their functions. This access is restricted by the firewall to internally initiated connections only.

17c. Examine use of "Little Snitch" application supervisor

Reference:
Little Snitch
Application Supervisor
Objective Development
URL: http://www.obdev.at/products/littlesnitch/index.html

Control Objectives:
Verify outbound traffic regulator is functioning correctly

Control Description:
Describe expected behavior of outbound traffic filter.

> *Little Snitch runs in the background and hooks into the operating system kernel while you are logged in. When an application tries to establish a network connection, Little Snitch intercepts the attempt and brings up an alert panel, telling you all the connection details including the name of the application which initiated the connection. You can either allow the connection, deny it or add a permanent rule for similar future-connections.*[21]

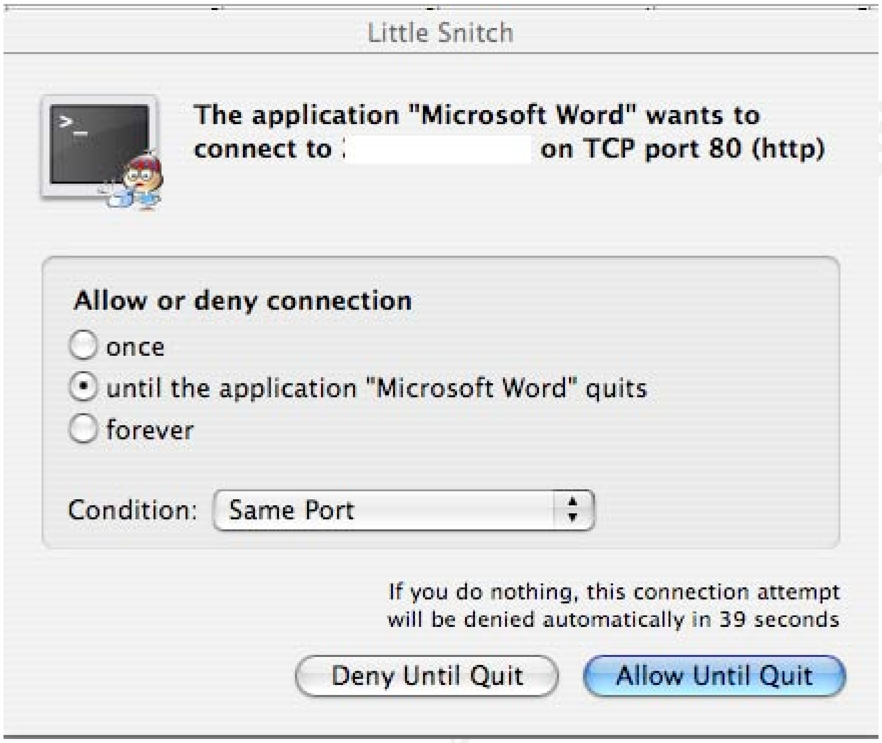
"Little Snitch" is used to warn user of surreptitious outbound connection attempts such as would be made by "spyware"[22]

[21] URL: http://www.obdev.at/products/littlesnitch/index.html

[22] What is Spyware?
Spychecker.com
URL: http://www.spychecker.com/spyware.html

Potential Risks:
"Spyware" or other types of program transmitting confidential information to unknown destinations or recording behavior of system users without the system owner’s knowledge or concurrence.

Verify program function by demonstration
Attempt to invoke embedded URL from within this document:



The application "Microsoft Word" wants to connect to [redacted] on TCP port 80 (http)

Allow or deny connection

○ once
● until the application "Microsoft Word" quits
○ forever

Condition: Same Port

If you do nothing, this connection attempt will be denied automatically in 39 seconds

User is notified of outbound connection attempt by program. Logging of outbound connections is not performed according to system policy, therefore no log entries are generated. Program appears to be functioning as designed.

Comments
The decision to construct a ruleset for ipfw and bypass the included GUI firewall configuration utility was made when the system owner noticed that enabling the included apache webserver via the GUI services panel also, without notifying the operator, enabled inbound traffic on port 80. These two actions are apparently bound together, as closing the port via the firewall control GUI also disabled the webserver. There was no desire to share private web pages with the world, so this tight coupling was found to be unacceptable. It was necessary to construct an ipfw ruleset and to modify the system start routines to load the enhanced firewall rules, but the results justified the effort. There are several rules included that are considered to be standard firewall practice that are not installed by the default configuration provided by Apple such as the anti-spoofing rules and the stateful inspection of outgoing traffic. This is a major upgrade in protection, in the author's opinion, and rectifies major shortcomings in the default configuration. This assessment and technical evaluation verifies that the firewall is performing

as intended, with the exception of the log entries lost due to the extreme overload generated during testing, and the slight possibility of potential firewall compromise under extreme load conditions.

Risk Rating: (_X_) High (__) Moderate (__) Low
Justification of rating:
Risk rating is high due to potential system exposures in case of firewall compromise
ST&E: (_X_) Pass (__) Fail

18. Logging and Auditing
References:
SANS Advanced System Audit: UNIX Workbook pp 74-83
"A Security Analysis of System Event Logging with Syslog"
by Kenneth E. Nawyn, June 27, 2003.
URL: http://www.sans.org/rr/papers/index.php?id=1101
Logging considerations discussed in the SANS Institute Track 7 Auditing Networks, Perimeters and Systems course will also be included in the evaluation.
A modified version of the freely available shell script based log analyzer "logcheck" is used to examine system logs for interesting events.
Instructions for use of this utility are found in articles by:
Marius Schamschula
"How to Configure logcheck Under Mac OS X"
Version 1.2.5 - 20021124
URL: http://www.hmug.org/HowTos/logcheck.html
and by
Trevor Warren
"Intrusion Detection Systems, Part IV: Logcheck"
freeos.com
URL: http://www.freeos.com/articles/3540/

Control Objective
Verify that implementation of system logging and event reporting are in conformance with the stated needs of the organization and are functioning as expected.

Control Description
All events reported by operating system components are logged by syslog to the file /var/log/system.log. This logfile, along with designated application logs, is to be combined with application logs and searched for events of interest on a daily basis and then compressed and archived. The log parsing utility "logcheck'" is designed to search logfiles for interesting events which are characterized as "Hacking Attempts", Security Violations", or "Unusual System Events" under control of several configuration files which contain signatures of various log events. The utility is launched automatically once a day and is configured to email a report of findings to the system operator.

Potential Risks
Possibility of events of interest such as attempts at system compromise or system malfunction escaping notice of system operators for an unacceptable length of time is a risk of incorrectly configured or underperforming logging system.

Statements of Compliance:
(_False_) Automated audit logs are maintained for at least 1 year.
(_True_) Email activity is logged in syslog or similar manner.
(_True_) Auditing is configured to record backups.
(_True_) SU and/or sudo activity is logged.
(_True_) User log on/log off activity is logged .
The following minimum auditable information is recorded for each event:
(_True_) Date and time.
(_True_) User Code.
(_True_) Success/failure of event.
(_True_) Origin of requests (device, terminal, port, etc.).

===> WHO REVIEWS LOG FILES AND HOW OFTEN:
(_True_) Logfile analysis is automated and accomplished daily.
(_True_) Reports of anomalous activity are sent automatically to the system administrator.

18a. Examine system logging configuration
Examine /etc/syslog.conf

```
# $FreeBSD: src/etc/syslog.conf,v 1.13.2.2 2001/02/26 09:26:11 phk Exp $
#
#       Spaces are NOT valid field separators in this file.
#       Consult the syslog.conf(5) manpage.
# uncomment this to enable logging of all log messages to /var/log/system.log
*.*                                     /var/log/system.log
# uncomment this to enable logging to a remote loghost named loghost
#*.*                                    @loghost
```

Verify that system logging is appropriately configured
Verify that desired information is being logged to desired location by manual examination of logfiles using "tail -f /var/log/system.log"
Trigger various loggable events and verify appropriate log entries are being generated.

Notable events are logged to the file /var/log/system.log. Sample is included.

```
Mar 20 15:44:55 localhost com.apple.SecurityServer: uid 501 succeeded authenticating as user claudel (uid
501) for right system.login.screensaver.
Mar 20 15:44:55 localhost com.apple.SecurityServer: Succeeded authorizing right system.login.screensaver
by process /System/Library/CoreServices/loginwindow.app for authorization created by
/System/Library/CoreServices/loginwindow.app.
Mar 20 15:50:00 localhost CRON[830]: (root) CMD (/usr/libexec/atrun)
Mar 20 15:56:56 localhost com.apple.SecurityServer: authinternal authenticated user claudel (uid 501) for
right system.login.tty.
Mar 20 15:56:56 localhost com.apple.SecurityServer: Succeeded authorizing right system.login.tty by
process /usr/bin/sudo for authorization created by /usr/bin/sudo.
Mar 20 15:57:38 localhost sudo:  claudel : TTY=ttyp4 ; PWD=/Users/claudel ; USER=root ;
COMMAND=/sbin/ipfw -a list
Mar 20 16:10:00 localhost CRON[849]: (root) CMD (/usr/libexec/atrun)
Mar 20 16:10:00 localhost anacron[850]: Anacron 2.3 started on 2004-03-20
Mar 20 16:10:00 localhost anacron[850]: Normal exit (0 jobs run)
Mar 20 16:32:00 localhost CRON[861]: (root) CMD (   /usr/sbin/ntpdate -bvs > /dev/null 2>&1)
Mar 20 16:32:01 localhost postfix/pickup[865]: 8B1F53595D5: uid=0 from=<root>
Mar 20 16:32:01 localhost postfix/cleanup[866]: 8B1F53595D5: message-
id=<20040321003201.8B1F53595D5@Blossom.local>
Mar 20 16:32:01 localhost postfix/qmgr[421]: 8B1F53595D5: from=<root@Blossom.local>, size=571,
nrcpt=1 (queue active)
Mar 20 16:32:01 localhost postfix/local[868]: 8B1F53595D5: to=<claudel@Blossom.local>,
orig_to=<root@Blossom.local>, relay=local, delay=0, status=sent (mailbox)
Mar 20 16:42:16 localhost kernel: ipfw: 2800 Deny UDP x.x.x.x:49362 255.255.255.255:2222 out via en0
Mar 20 16:44:44 localhost /usr/libexec/fix_prebinding: /sw/bin/clear could not be launched prebound.
Mar 20 16:44:49 localhost /usr/libexec/fix_prebinding: /sw/lib/libncurses.5.dylib must be slid, but
fix_prebinding could not find a good place to relocate it.
Mar 20 17:38:04 localhost com.apple.SecurityServer: authinternal failed to authenticate user claudel for right
system.login.tty.
Mar 20 17:38:04 localhost com.apple.SecurityServer: Failed to authorize right system.login.tty by process
/usr/bin/sudo for authorization created by /usr/bin/sudo.
Mar 20 17:38:09 localhost com.apple.SecurityServer: authinternal authenticated user claudel (uid 501) for
right system.login.tty.
Mar 20 17:38:09 localhost com.apple.SecurityServer: Succeeded authorizing right system.login.tty by
process /usr/bin/sudo for authorization created by /usr/bin/sudo.
Mar 20 17:38:09 localhost sudo:  claudel : TTY=ttyp4 ; PWD=/Users/claudel ; USER=root ;
COMMAND=/bin/ls -al /
```

Comments

A random sampling of logged events shows that the system logger is writing entries to the system logfile /var/log/system.log as expected. Authentication successes and failures are appropriately logged, as are other manually triggered events. Packets rejected by the firewall are correctly logged, as are a number of routine events such as transmission of email by the "postfix" Mail Transport Agent and the invoking of various tasks by the system utility "cron". During the firewall evaluation a number of log entries were truncated, probably due to events being generated faster than the system could write them to the logs. Examples of truncated log entries are included in the system traffic control evaluation section.

Special note

In the course of this evaluation the author noticed a pattern of denied packets being logged by the system firewall such as this sample.

```
Mar 20 16:42:16 localhost kernel: ipfw: 2800 Deny UDP x.x.x.x:49362 255.255.255.255:2222 out via en0
```

The pattern consists of packets transmitted from the system on a incrementing high-numbered port with a broadcast destination of 255.255.255.255:2222. Port 2222 is listed by IANA as being assigned to "rockwell-csp2". A cursory Internet search provided little information on the intended usage of this port. More interesting to the author was the discovery that the appearance of this particular pattern apparently coincides with the launching of any of the programs included in the Microsoft Office X suite of applications. Excel, Word, Power Point, and Entourage all seem to attempt to broadcast a few packets at startup, and again at random intervals while the program(s) are running. MS Virtual PC also attempts a broadcast, but to the same destination port as the source port rather than to port 2222. A sampling of this behavior was captured with the network traffic analyzer "ethereal[23]", but the author was unable to decode the contents of the transmitted packets. On program exit Word issues a message "Word is attempting to connect to the printer". The timing of this message coincides with a log entry as described earlier in this section. No printing problems are noted as a result of dropping this traffic. This phenomenon turns out to be an anti-piracy scheme that checks for duplicate registration numbers on the local subnet[24].

18b. Verify firewall logging by examining logs produced during firewall test.
Were all scans/probes detected and logged?
Were any events missed?

Probably. Some log entries were truncated, presumably due to scan overloading the firewall/logging subsystem. Evaluator was unable to make a one to one correspondence between specific tests and expected log results. Approximately 50Mb of logs were generated during scans, consisting mostly of entries for denied packets.

Were any logging thresholds reached?

Yes, logging threshold of 100000 entries/rule was reached on the deny-all rule #2900 during initial test, and was temporarily raised to 1000000 for the remainder of the scan tests

Interesting log entries from /var/log/system.log generated during the scans

```
Mar 27 01:12:57 Blossom xinetd[284]: START: pop3 pid=618 from=x.x.x.x
Mar 27 01:12:57 Blossom xinetd[618]: FAIL: pop3 address from=x.x.x.x
Mar 27 01:13:01 Blossom kernel: Limiting closed port RST response from 271 to 250 packets per
second
Mar 27 01:26:27 Blossom kernel: Limiting icmp unreach response from 331 to 250 packets per
second
Mar 27 01:30:59 Blossom kernel: icmp_error: bad length
Mar 28 10:30:13 Blossom kernel: ipfw: 1900 Accept TCP y.y.y.y:20 x.x.x.x:8888 in via en0
Mar 28 10:30:13 Blossom kernel: ipfw: 1900 Accept TCP x.x.x.x:8888 y.y.y.y:20 out via en0
Mar 28 10:34:04 Blossom kernel: attempted source route from y.y.y.y to x.x.x.x
Mar 28 10:34:04 Blossom kernel: icmp_error: bad length
Mar 28 10:37:34 Blossom kernel: .28 x.x.x.x in via en0 (frag 30416:1144@2960)
Mar 28 10:52:51 Blossom kernel: attempted source route from y.y.y.y to x.x.x.x
```

[23] Ethereal.com
"Introduction"
URL: http://www.ethereal.com/introduction.html

[24] United States Government Department of Energy
Computer Incident Advisory Capability (CIAC)
CIACTech02-003: "Protecting Office for Mac X Antipiracy Server Ports"
April 26, 2002 00:00 GMT
Revised: 7 May 2002
URL: http://www.ciac.org/ciac/techbull/CIACTech02-003.shtml

Examples of truncated log entries.

```
Mar 28 10:41:59 Blossom kernel: .6:52832 in via en0
Mar 28 10:42:00 Blossom kernel: y.y.y.y:59397 x.x.x.x:52832 in via en0
Mar 28 10:42:01 Blossom kernel: 68.1.6:52832 in via en0
Mar 28 10:42:02 Blossom kernel: .6:52832 in via en0
Mar 28 10:42:03 Blossom kernel: 2832 in via en0
Mar 28 10:42:04 Blossom kernel: 2.168.1.6:52832 in via en0
Mar 28 10:42:05 Blossom kernel: 832 in via en0
Mar 28 10:42:06 Blossom kernel: n0
Mar 28 10:42:07 Blossom kernel: 52832 in via en0
Mar 28 10:42:08 Blossom kernel: x.x.x.x:52832 in via en0
Mar 28 10:42:08 Blossom kernel: via en0
Mar 28 10:44:18 Blossom kernel: eny ICMP y.y.y.y x.x.x.x in via en0 (frag 43778:1472@25024+)
```

18c. Examine use of "logcheck" system log utility.

Describe expected behavior of log event reporting subsystem
The log parsing utility "logcheck'" is designed to search logfiles for interesting events which are characterized as "Hacking Attempts", Security Violations", or "Unusual System Events" under control of several configuration files which contain signatures of various log events. The utility is launched automatically once a day and is configured to email a report of findings to the system operator.

Verify program is automatically launched on appropriate schedule.
Verify notifications by visual inspection of mailbox.
Do reports arrive at appropriate time?

Verify logcheck is correctly categorizing results by examination of mailed report:

Examination of emailed reports indicates that the logcheck utility is being run at the desired time. Appropriate characterizations of reportable events as "Security Violations" (Denied IP traffic, failed authentications) or "Unusual System Events" are included. No events characterized as "Hacking Attempts" were logged during the evaluation. The logcheck report from logs generated during this evaluation overloaded the host's email system due to its abnormally large size and was not delivered. It is extremely unlikely that a similar quantity of log entries would ever be generated in normal operation.

Section of daily logcheck report:

```
Security Violations
=-=-=-=-=-=-=-=-=-=
Mar 22 08:42:18 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:23922 x.x.x.x:135 in via en0
Mar 22 08:42:18 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:0 x.x.x.x:22 in via en0
Mar 22 08:42:18 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:742 x.x.x.x:515 in via en0
Mar 22 08:42:18 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:37672 x.x.x.x:23 in via en0
Mar 22 08:42:19 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:16394 x.x.x.x:21 in via en0
Mar 22 08:42:20 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:0 x.x.x.x:1917 in via en0
Mar 22 08:42:21 localhost kernel: ipfw: 1400 Deny TCP y.y.y.y:61689 x.x.x.x:80 in via en0
Mar 22 08:42:21 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:64657 x.x.x.x:1 in via en0
Mar 22 08:42:21 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:64658 x.x.x.x:2 in via en0
Mar 22 08:42:21 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:64667 x.x.x.x:11 in via en0
<snip for brevity>
Mar 22 08:45:58 localhost kernel: ipfw: 2700 Deny TCP y.y.y.y:4865 x.x.x.x:49442 in via en0
Mar 22 09:31:16 localhost kernel: ipfw: 700 Deny TCP attempted source route from y.y.y.y to x.x.x.x
Mar 22 09:31:16 localhost kernel: ipfw: 600 Deny TCP icmp_error: bad length
Mar 22 09:31:21 localhost kernel: ipfw: 700 Deny TCP attempted source route from y.y.y.y to x.x.x.x
Mar 22 09:31:21 localhost kernel: ipfw: 600 Deny TCP icmp_error: bad length
Mar 22 20:30:07 localhost com.apple.SecurityServer: authinternal failed to authenticate user claudel for right
system.login.tty.
Mar 22 20:30:07 localhost com.apple.SecurityServer: Failed to authorize right system.login.tty by process
/usr/bin/sudo for authorization created by /usr/bin/sudo.

Unusual System Events
=-=-=-=-=-=-=-=-=-=-=
Mar 20 08:45:57 localhost kernel: From path: "/pci@f2000000/mac-io@17/ata-
4@1f000/@0:5,\mach_kernel", Waiting on <dict ID="0"><key>IOPathMatch</key><string
ID="1">IODeviceTree:/pci@f2000000/mac-io@17/ata-4@1f000/@0:5</string></dict>
Mar 20 10:13:04 localhost kernel: en0: promiscuous mode enabled
Mar 20 10:13:04 localhost kernel: en0: promiscuous mode disabled
Mar 20 20:42:05 localhost crashdump: Started writing crash report to:
/Users/claudel/Library/Logs/CrashReporter/Microsoft Word.crash.log
Mar 20 20:42:08 localhost crashdump: Finished writing crash report to:
/Users/claudel/Library/Logs/CrashReporter/Microsoft Word.crash.log
```

Verify appropriate archiving of logs and notifications by visual examination. Include sample directory listing

```
{root@blossom:/var/log/logchecks:44}ls -al 03.20.2004
total 44
drwx------   4 root  wheel    136 20 Mar 00:16 .
drwxr-xr-x  22 root  wheel    748 20 Mar 00:16 ..
-rw-------   1 root  wheel  37772 20 Mar 00:16 03.20.2004-00.16.log.gz
-rw-------   1 root  wheel   1671 20 Mar 00:16 03.20.2004-00.16.rpt.gz
```

Combined logfiles and emailed report are archived in appropriate subdirectory

Comments

Logging subsystem is performing as expected. Events are normally logged as required by policy, and the logs are examined daily for anomalous events. The logs are not encrypted, but no significant risk is incurred by this lack in this instance. It is possible to overload the logging system with data generated by extreme port scans, but this is not anticipated to be a frequent occurrence and the symptoms of overload are a warning of unusual events in any case. Reports are created and sent automatically to the system administrator on a daily basis. This level of reporting would probably be insufficient to allow speedy response in case of system compromise. More frequent running of the "logcheck" utility would provide a more timely warning of possible system attacks or compromise, but increased frequency of reporting has not been deemed necessary in this case. Raw logs are archived daily and are available for any needed forensic analysis. Archived logs are removed from the system on an irregular schedule to conserve disk storage. Frequent tuning of logcheck configuration files is needed to assure complete and accurate reporting of logged events of interest.

Risk Rating: (__) High (_X_) Moderate (__) Low
Justification of rating:
Risk rating is moderate due to possibility of missed events
ST&E: (_X_) Pass (__) Fail

19. MacAnalysis for OS X
Control Objectives:
Provide alternate to nessus vulnerability scanner

Control Description:
MacAnalysisX is a vulnerability scanner specifically designed for OS X.
Full description of program is at manufacturers website:
URL: http://www.macanalysis.com/about.php3

Include and interpret results

MacAnalysis Started at: 8:27 PM

MacAnalysis scans over 1600 holes, please do something else during the scan.
For more informations: support@macanalysis.com

STEP 1: CGI vulnerabilities
CGI Vulnerability found: nlog-smb.pl .
Reveals system information. (Risk: Low)

STEP 2: Folders:
Viewable Folder found: /images .
Viewable Folder found: /manual .

STEP 3: Trojans

STEP 4: Services/Protocols Holes

STEP 5: Remote Procedure Call

STEP 6: CGI syntax

```
MacAnalysis 2.0b: 127.0.0.1 Port scan
Wed Mar 17 09:43:15 PST 2004
80      Active      www-http - World Wide Web HTTP
110     Active      pop3 - Post Office Protocol - Version 3
631     Active      Unknown
10025   Active      Unknown
10110   Active      Unknown
```

Investigate all findings

80   Active   www-http - World Wide Web HTTP
Active ports on webserver
110   Active   pop3 - Post Office Protocol - Version 3
POP Server

```
#grep 631 /etc/services
ipp          631/udp     # IPP (Internet Printing Protocol)
ipp          631/tcp     # IPP (Internet Printing Protocol)
```

Common UNIX Printing Service
Web service, POP service and CUPS print service are all restricted to localhost access by configuration and by firewall rules.

```
#lsof |grep 10025
ssh 24465 claudel 6u IPv6 0x02979cd0 0t0 TCP localhost:10025 (LISTEN)
ssh 24465 claudel 7u IPv4 0x02faa9f8 0t0 TCP localhost:10025 (LISTEN)
```

SSH Tunnel to ISP SMTP server

```
#lsof | grep 10110
ssh 24465 claudel 4u IPv6 0x02979e80 0t0 TCP localhost:10110 (ESTABLISHED)
ssh 24465 claudel 5u IPv4 0x02f6d4c8 0t0 TCP localhost:10110 (LISTEN)
```

SSH Tunnel to ISP POP server

Investigate and resolve all differing findings between MacAnalysis and the Modified NSWC Checklist Results

MacAnalysys identified an open port, #631 belonging to the Common Unix Printing System that was overlooked/ignored by the nessus scan. Access to this port is restricted to the local system. It is possible that this was due to the printer being turned off during the nessus scans. This is an insignificant oversight. Nessus identified several open ports/running services that were not noted by MacAnalysis, but that is because the services identified by nessus were in use by nessus and were not active during the MacAnalysis scan. CGI vulnerabilities are outside the scope of the investigation, but are not accessible from the outside in any case.

20. Assess potential risk to this system from any of the current SANS Top 10 UNIX vulnerabilities

U1 BIND Domain Name System
BIND server not in use, DNS client usage only.
Verified by issuing command
ps ax | grep named and not seeing named running
named binary disabled by issuing command
chmod -x /usr/sbin/named
ls -al /usr/sbin/named
-rw-r--r-- 1 root wheel 1252248 15 Mar 15:24 /usr/sbin/named

U2 Remote Procedure Calls (RPC)
Disabled.
Verified by examining listing of active system processes and by nessus scan.
Inbound ports are blocked by packet filter
Binaries have been disabled by removing execute permission
sudo chmod -x /usr/sbin/portmap

```
ls -al /usr/sbin/portmap
-r--r--r--  1 root  wheel  38400 15 Mar 15:24 /usr/sbin/portmap
sudo chmod -x /usr/sbin/rpc*
ls -al /usr/sbin/rpc*
-r--r--r--  1 root  wheel  64796  5 Mar 16:10 /usr/sbin/rpc.lockd
-r--r--r--  1 root  wheel  26168  5 Mar 16:10 /usr/sbin/rpc.statd
-r--r--r--  1 root  wheel  19116 15 Mar 15:24 /usr/sbin/rpcinfo
```

U3 Apache Web Server
In use
Restricted by configuration to localhost access.
Inbound http/https ports blocked by firewall.
Verified by examination of configuration files and by nessus scan.

U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords
All service accounts have default login shells set to /dev/null or /usr/bin/false.
Verified by examination of netinfo database.
Operational accounts have strong passwords.
Verified by examination only.

U5 Clear Text Services
Policy prohibits use.
SSH is in use for outbound communication.
Inbound connections are not generally permitted.
Verified by examination of configuration files, running processes, and by nessus scan.

U6 Sendmail
Not used
Postfix is the MTA of choice for OS X 10.3 and later.
Incoming SMTP port is blocked. All SMTP traffic travels thru SSH tunnel.
Verified by examination of configuration files, running processes, and by scan.

U7 Simple Network Management Protocol (SNMP)
Disabled/blocked.
Verified by examination of configuration files, running processes, and by nessus scan.
Binary for snmp daemon is disabled by removing the execute permission

```
sudo chmod -x /usr/sbin/snmpd
ls -al /usr/sbin/snmpd
-rw-r--r--  1 root  wheel  43700 12 Sep  2003 /usr/sbin/snmpd
```

U8 Secure Shell (SSH)
Use of SSH version 1 is subject to vulnerabilities described at
URL: http://www.sans.org/top20/#u8
or at
URL: http://www.ssh.com/company/newsroom/article/212/

Usage of SSH protocol version 1 for communication with their ISP is forced on the target organization until their ISP upgrades the available protocols to version 2. SSH use is limited to that of client only, and appropriate precautions as described in the advisory are in use. The service daemon is not enabled on this system and the commonly used port, 22, is blocked for inbound traffic by the system firewall. This is verified by examination of running process listings, by scanssh, and by nessus scans.

```
ps waux | grep ssh
claudel 20895   0.0  0.0     8860      8 std  R+    11:31AM   0:00.00 grep ssh

scanssh x.x.x.x
x.x.x.x <refused>

scanssh 127.0.0.1
127.0.0.1 <refused>
```

Version of SSH in use on the target system is verified by issuing the command "ssh -V" at a shell prompt.

```
ssh -V
OpenSSH_3.6.1p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL 0x0090702f
```

This version is the most recent Apple has released via "Software Update" and will be presumed to be free of any known exploitable vulnerabilities. Detailed evaluation of OpenSSH is beyond the scope of this investigation.

U9 Misconfiguration of Enterprise Services NIS/NFS
NIS/NFS disabled on this system
Verified by examination of configuration files, running processes, and by nessus scan.

binaries have had the execute permission bit unset

```
sudo chmod -x /sbin/nfsd
ls -al /sbin/nfsd
-r--r--r--  1 root  wheel  15600  5 Mar 16:10 /sbin/nfsd
```

U10 Open Secure Sockets Layer (SSL)
OpenSSL, while subject to various vulnerabilities, is currently at the most recent available stable release

```
openssl version
OpenSSL 0.9.7d 17 Mar 2004
```

Comments
The three services included in the SANS "top10" that are in use on this system are used in a manner that will minimize potential exposure. The apache webserver in use is restricted by configuration and the inbound port access is blocked at the firewall. SSH daemon is not in use, only the client portions of the utility, which are subject to the same vulnerabilities as the server. SSH client is used to establish only encrypted sessions, which will reduce potential exposure. Use of the latest available version minimizes vulnerabilities of OpenSSL usage. The remaining risky services have been disabled. Disabled binaries need to be manually checked after system updates for reenabled execute permissions.

Risk Rating: (_X_) High (__) Moderate (__) Low
Justification of rating:
High risk due to popularity of these vulnerabilities
ST&E: (_X_) Pass (__) Fail

Final comments and explanations
are included in Assignment 4

Risk Assessment Completed By (Primary User):

Neatly Printed Name: Claude V. Lucas
Common ID:____________________________________
Phone Number:_(_____)___________________________
Signature:______________________________________
Date:____

As part of the Security Test & Evaluation, I verify that all applicable vendor recommended Security Related patches are installed and up to date on this IS.

ST&E Completed By:

Neatly Printed Name: Claude V. Lucas
Common ID:____________________________________
Phone Number:_(_____)___________________________
Signature:______________________________________
Date:____

Assignment 4: Follow Up

Introduction

In this assignment, the results of the evaluation performed for Assignment 3 will be interpreted, and assessment of risks will be presented along with the evaluator's findings and recommendations for improving the security of the target system.

Executive Summary

The United States Government's National Security Agency has provided an unclassified Information Security Assessment Methodology (NSA-IAM) intended for the use of the general public. The intent of this methodology is to facilitate an improvement of the overall level of security on the public networks by providing a flexible and thorough infosec assessment framework. The mission of the target organization is to provide a variety of Information Technology consulting services to a variety of clients. An assessment and technical evaluation of the portable Apple PowerBook system in use was performed in order to provide material to satisfy requirements of the GIAC Certified System Auditor practical assignment, and to validate system operations and configuration for the benefit of the system owner. A secondary purpose for this exercise is the creation of an IAM checklist and an OS X checklist that may be of future use to both the author and the community at large. The use of the IAM to assess a single portable workstation may appear to be excessive, but the methodology is scalable and is effective regardless of the size of the organization under assessment.

In some instances, program listings such as the contents of the /etc/periodic directories, and test results such as the full nmap scan results were not included in the report. This omission is intentional and for the purpose of brevity. In a "real world" assessment, these listings and raw test results would certainly be included.

This system, for the most part, is configured and operated in as secure a manner as is possible for this type of system. Potential exposure, in terms of critical vulnerabilities, is minimized by appropriate safeguards that are described in the body of this report. Shortcomings and potential solutions are presented in the "conclusions" section of this assignment.

Were assessment and evaluation objectives met?

The objective of this assessment and evaluation is to provide assurance that the target system is being operated in the most secure manner possible within the constraints of budgetary and operational necessities. An additional objective is to construct an assessment and evaluation checklist that will be usable as a starting point for future evaluations of other systems.

These objectives were both met in the course of creating this report.

System Description
A portable single user endpoint Apple PowerBook system operating under OS X "Panther" version 10.3.3 that is utilized in a variety of circumstances ranging from hotel room dialup or broadband access, public wireless access points, to highly secured installations.

Critical Vulnerabilities:
Potential risks to the information contained in this target system consist of the following:
Loss of availability of data due to hardware malfunction
Loss of entire laptop system from theft
Loss or corruption of data due to operator error
Loss of control over system or compromise of information confidentiality, integrity, or availability due to possible unauthorized activities of third parties

Review of the Assessment Process
The US Government National Security Agency's Infosec Assessment methodology was interpreted by the author and applied to the target system and associated operational practices. This assessment revealed areas that would benefit from technical evaluation. Evaluation of OS X operation and configuration, with an emphasis on network traffic controls and on the logging subsystem was performed using a modified version of the Naval Surface Warfare Center's OS X evaluation checklist. A mix of observation of system operations, examination of various system configuration files, and technical evaluations led to and validated the findings presented in this report.

Final analysis in terms of the 18 NSA-IAM baseline categories

Management Aspects
1. INFOSEC Documentation
No effective documentation regarding the specific configuration of the target installation exists. There is some specific configuration information in a text file (~./Documents/misc/mac-hints.txt) but it is not comprehensive. No written security policies, procedures, standards documentation or requirements documentation exists in this case. Documentation for various application programs and system utilities exists as printed books or web bookmarks pointing to various Internet sites. There are no mandatory documentation standards being followed and there is no stated policy requiring any documentation whatsoever. This area is in need of improvement as time permits.

2. INFOSEC Roles and Responsibilities
This particular organization is a "one man shop" with all roles and responsibilities filled by the same individual.

3. Contingency Planning

There are no written contingency plans for this organization. Catastrophic hardware failure is covered by an extended maintenance plan with the vendor (AppleCare Protection Plan). Validity of the maintenance contract was confirmed by a phone call to the vendor. Although formal technical evaluation of the existing backup scheme has not been performed for this exercise, the scheme has been tested by the system owner and has been found to be adequate.

4. Configuration Management

No written configuration management policies are in force in this organization due to the extremely limited size of the organization. This is an area in need of improvement, as few records of various system configuration settings exist other than in the running system.

Technical Aspects

5. Identification and Authentication

Identification and authentication are accomplished by means of the default vendor provided UNIX based login procedure. Local account information is locally stored in the "netinfo" database, with a user ID (uid) and group ID (gid) assigned at the time of account creation. In the case of this particular target, I&A is not a major concern due to the single-user nature of the organization and system. A reasonably secure (8+ character, non dictionary, upper and lower-case characters, numbers & special characters) password is in use to permit system access. Unfortunately, due to the lack of built in password controls except in the server version of OS X there are no automatic mechanisms to enforce password length or expirations. This is not a significant exposure in a single-user system where the owner/user chooses the password wisely and periodically changes it.

6. Account Management

There is only one interactive account other than the system default accounts in use on this computer. Several non-interactive accounts are in use to allow functioning of various applications. These accounts are rendered incapable of allowing interactive access by setting the default shell to either /dev/null or /usr/bin/false. This will remain the practice for the foreseeable future. Therefore, account management is not a high priority issue for this organization.

7. Session Controls

Due to the single user nature of this system, the only session control deemed necessary is the implementation of a password-controlled screen saver. (SereneScreen Marine Aquarium V2.0[25]) which is set to activate at times ranging from 5 minutes to never, depending on the location of the system and any activities in progress. The screensaver is also instantly activated by means of a "hot corner".

[25] SereneScreen.com
"SereneScreen Marine Aquarium 2 - Mac OS X"
URL: http://www.serenescreen.com/product/maquariumx/

8. External Connectivity

Internet Usage

Most of the ongoing usage of this system involves the Internet. Research, email correspondence, and the safe conduct of daily business are all concerns of the system owner. The system in question is often connected to the Internet and left in an unattended state by the operator. There are no written policies in place regarding use of the Internet. Unwritten system policy insists that all usage of the Internet will be conducted in a manner that will not expose sensitive information to inadvertent or purposeful unauthorized disclosure or alteration and all usage of the Internet will be conducted in a manner that will not allow third parties to use or access system assets. There are traffic control entities (firewalls) in place on the target system to enforce these policies, and their proper function has been verified by technical means and by observation of function in section 17 of the modified NSWC checklist. This evaluation was purposefully limited to nmap and nessus scans. Confidentiality is protected by the use of OpenSSH and its tunneling capability to encrypt all transmissions other than HTTP/HTTPS to and from the ISP.

Modems

Modem usage policy and practice in this installation mirrors the broadband usage described in the previous section.

Dedicated line

There are no dedicated communication links in use.

Wireless connectivity

Wireless connectivity usage policy and practice in this installation also mirrors the broadband usage described in the previous section. System is used as a wireless client only and is not used as a wireless Access Point.

9. Telecommunications

No additional telecommunications facilities are in use in this organization.

10. Logging and Auditing

UNIX derived syslog facility is used to record all significant system events to a logfile in the system directory /var/log/system.log. This log, along with the httpd daemon error log are parsed once daily by means of the utility script "logcheck", which has been modified to include a log archiving capability. Interesting results are then mailed to the system operator. Logs are recycled daily and archived into a subdirectory of the system log directory. Logging and reporting of events has been validated for this client by thorough examination. This examination is described in section 18 of the modified NSWC checklist, including the logging failure induced during the firewall evaluation by inducing extreme numbers of rejected packets.

11. Virus/Malware Protections

The Apple OS X operating system has been, to this point in time, remarkably free of malicious code. This happy circumstance is not expected to be a long-term trend, and the system owner has established Internet Usage procedures to minimize the chance of allowing email-vectored malware to enter the system. Before downloading email, the system operator logs into a shell account provided by the client's ISP and examines all incoming email with the standard UNIX email client "mutt". Unsolicited suspicious correspondence is deleted at that point, never reaching the laptop system. However, use of anti-virus software on the OS X host is indicated in order to prevent the inadvertent transmission of infected code to susceptible systems. The Microsoft Windows subsystem running under Microsoft's Virtual PC is a different story. The risks to MS Windows installations are well known and too numerous to tabulate here. Minimal due care in the form of Symantec Corporation's Norton AntiVirus, which is installed and configured to automatically download profile updates, and a policy of frequent visits to the MS Windows update site are in place, along with a policy of disabling all unneeded Windows services. This has been deemed adequate protection of the Windows subsystem from malware for this particular installation. Purchase and installation of a native OS X anti-virus scanning product is indicated. In the course of this assessment, a major oversight on the part of the system owner was discovered. In order to protect the system against surreptitiously replaced system binaries, industry standard safe practice indicates use of a checksumming utility such as Tripwire. In this case, no such practice was followed and, theoretically, the system was and is subject to potential compromise. It is the opinion of the owner/assessor that this particular target is not valuable enough to attract a targeted attack of this nature, and that the labor involved in reinstalling the operating system, applications, and user files for the purpose of guaranteeing a "clean" installation and then establishing a baseline of checksums is not cost-effective in this particular instance. Running a check for "rootkits" is indicated as soon as a reliable rootkit scanner can be found.

12. Maintenance Activities

Software upgrades and patches are normally installed as soon as they become available. This was verified in the technical evaluation under section 5 of the modified NSWC checklist. Apple upgrades are installed via the "System Update" facility. Open Source updates are installed via the Fink project utilities, in most cases. Mission critical Open Source applications such as ethereal and nessus are maintained by the system owner outside of the Fink project area. It is an established practice to update the MS Windows subsystem on a weekly basis via the included "System Update" utility. Apple performs hardware maintenance as needed under a maintenance contract. System owner subscribes to Apple, SANS and CERT alert mailing lists to assure prompt notification of any new vulnerabilities as they are discovered.

13. Backup/Recovery

System backup is generally performed on an ad hoc basis by cloning the system drive to an external 120Gb firewire hard drive with multiple partitions, which allows several full backups to be kept. Bombich Software's Carbon Copy Cloner[26] is used to make an exact copy of the system disk to an external partition. This external drive is normally stored in a separate location from the

[26] Bombich Software
"Carbon Copy Cloner"
URL: http://www.bombich.com/software/ccc.html

target system when not in use. The resulting clones are fully bootable, and booting on one and using it in normal operation has proved viable operation from a cloned disk. Additional backup of user files is accomplished as necessary via Roxio System's Toast[27] DVD/CD writing utility and the target system's SuperDrive DVD/CD burner. Due to the irregular nature of the operation and use of this system, regularly scheduled backups are considered superfluous. Full system backups are generally done before any major configuration changes, and are done bi-weekly in any case. Interestingly enough, a variant of this backup scheme is beginning to become acceptable practice for much larger installations.

Operational Aspects:

14. Labeling/Classification of data

No data classification schemes are in use or needed by this organization. All information is presumed to be of the highest importance and is guarded accordingly, within budgetary and operational constraints.

15. Media sanitization and disposal

Expired media such as obsolete DVD/CDs are physically destroyed manually before disposal in the trash. Purchase of a capable shredder when budget allows is indicated.

16. Physical security

Theft of portable computing systems is a major threat to the security of the target. Vigilance on the part of the owner, along with a cable lock[28] is the first line of defense.

17. Personnel Security

Personnel Security is not a critical issue in a one-person shop and will be ignored for the purpose of this report.

18. Training and security awareness

In this instance, there are no specific training or security awareness procedures in place, but there is a definite commitment to ongoing education.

Conclusions

Traffic control and logging procedures have been examined in assignment 3 as part of the modified NSWC checklist and found to be consistent with industry defined "best practices" and with the needs of the system owner. Some typical system tasks such as email retrieval through the SSH tunnel and "web surfing" were performed during the extreme external firewall scans without noticeable problems. This leads to the conclusion that the system is to some degree immune to a denial of service attack involving extreme levels of inbound traffic.

[27] Roxio, Inc.
“Toast Titanium”
URL: http://www.roxio.com/en/products/toast/index.jhtml

[28] Kensington Technology Group
“MicroSaver Security Cable”
URL: http://www.kensington.com/html/2219.html

The fact that the logging subsystem was overloaded during the firewall test as described in section 18b of the modified NSWC checklist does not lead the author to conclude that there is an elevated risk of a similar failure happening during normal operations. Software updates are applied promptly. Effective email screening procedures minimize the possibility, however remote, of viral infection and retransmission. Existing backup and recovery procedures, while basic, have been proved an acceptably viable and effective guard against inadvertent, accidental or malicious threats to information CIA. The most critical shortcoming found is the lack of file checksumming software that could possibly facilitate or help to hide a system compromise. The purchase of native OS X anti-virus software is indicated to further reduce the remote possibility of infection or retransmission of infested files. The software cost to mitigate these two shortcomings is small in terms of dollars, but the time investment to properly install file integrity checking software is prohibitive at this time. This will be remedied at the next full reinstall of operating system software. System documentation is another area in need of improvement. Installation of an Intrusion Detection System for operational, rather than experimental purposes would probably not be cost or time effective given the proved solid nature of the system firewall configuration. Identification and authentication measures in use, while probably inadequate for larger systems, are adequate in this instance. Likewise, configuration management and documentation practices that would be woefully insufficient in a larger organization are tolerable in this case.

What was not validated?

Backup and Recovery

Backup and recovery procedures were tested by the means of booting on a cloned external drive and performing a cursory examination of system function. This test, while encouraging, is not a complete test of the reliability of the backup. A higher degree of certainty would be achieved by initializing the internal hard drive, booting on the backup, cloning the backup to the internal drive and resuming normal operations.

Service account vulnerabilities

Illicit access via non-interactive service accounts was not attempted. No passwords have been created for these accounts, and disabling the default shells is presumed to be effective.

Behavior of ipfw packet filter under extreme stress conditions

During the technical evaluation the included packet filter "ipfw" and/or the logging system showed possible symptoms of failure while undergoing intense scanning from an external source such as truncated log entries. A deeper evaluation of Apple's ipfw implementation was both outside the scope of this general system evaluation and not possible due to lack of hardware resources of the examiner. A more intense scrutiny of the firewall would require bombardment of the system with a larger variety of input stimuli than was used in this evaluation from more discrete sources than were available for this test. There was only one machine other than the target system available for testing purposes during this evaluation and the author would choose to use more than one "attacker" concurrently for a complete firewall evaluation.

Configuration error found during and corrected during writing of practical.
While finishing this practical, the author noted that all the firewall rules were not being installed when the system was started in "stand-alone" mode and there was no active ethernet connection present. Investigation of this disturbing discovery found that the misbehavior was due to the rules

```
# Allow SSH traffic <> ISP without state inspection or logging
add allow tcp from any to <isp.net> 22 out
add allow tcp from <isp.net 22> to any in
```

referencing an internet location by name. Without an active connection, name resolution was disabled and ipfw refused to load the this rule or the rules following it, creating a ruleset that was allowing almost all traffic to pass via the OS X "default allow" rule. This misconfiguration was immediately corrected by hardcoding the "isp.net" IP address into the offending rules. Rebooting the system and examining the running firewall with the "ipfw -a list" command tested and proved the fix.

In all honesty, the author cannot claim that this discovery was due to the execution of any of the assessment or evaluation plans, which completely omitted the testing of any of the system components without the presence of an active ethernet connection. Discovery occurred while using a dialup connection from a hotel when the author, on a serendipitous whim, decided to check the firewall rules while connected via a PPP connection. If anything, this discovery proves both the ease of improperly configuring essential system components, and the difficulty involved in "covering all the bases" while crafting assessment and evaluation plans.

Residual risks:
Possibility of infection or propagation of malicious code
Due to lack of anti-virus protection, there is a slight risk of inadvertent retransmission of malicious code to vulnerable external systems in case of lapse of operator vigilance. There also is a slight risk of viral infection by yet unreleased OS X virus. Purchase of OS X anti-virus product is indicated to mitigate this exposure.

Target system is subject to the introduction of altered system binaries.
This risk, while a theoretical possibility, is not considered likely due to the practices of frequent system updates and rigorous traffic control. Installation of file integrity checking software is indicated to help remediate this exposure. Also, deployment of a reliable "rootkit" detector if any become available would be another mitigating factor.

Software Update facility enables disabled features
Apple's Software Update procedure exhibits the rude behavior of reinstalling and re-enabling operator disabled processes. It is necessary to examine the system and re-disable NFS/RPC, portmapper, named, and other operator disabled processes after system software upgrades. NFS is disabled on this system by removing the startup scripts and plists from the system directory /System/Library/StartupItems. Removing “execute” permissions from the binaries disables other questionable programs.

Possibility of a third party hijacking the Apple System Update facility
This is a risk of low probability, but greater than zero possibility. Remediation is a matter of Apple increasing the security of the System Update process to reduce the likelihood of a third party spoofing the location of the update server and is beyond the control of the customers. This risk has been partially remediated in this system by configuring "Little Snitch" to allow the System Update facility to only access certain locations that are known to be authentic.

Potential exploitation of yet undiscovered vulnerabilities in UNIX services
This is an ongoing risk in the operation of all UNIX based systems. Remediation is accomplished by prompt installation of system updates and by vigilant monitoring of various infosec mailing lists.

Race condition noted at system startup
During system startup there is a brief period before the ipfw rules are loaded that the "default allow" rule #65535 "allow ip from any to any" is the only rule in effect. This is apparently due to the boot process issuing the "ifconfig" command and enabling the network interface before loading the firewall rules. The evidence for the problem is the traffic logged by the default allow rule. A number of packets are logged to this rule, as seen by issuing the "ipfw -a list" command, but the number does not continue to increase over time after ipfw rules are loaded. In OS X, the kernel configuration parameter "IPFIREWALL_DEFAULT_TO_ACCEPT" which allows all traffic to pass by default is enabled in the Apple provided kernel. It should be possible to construct a customized kernel from source code and disable this feature, but the costs in effort required are prohibitive for this system. Apple occasionally includes a new kernel with some software updates, which would necessitate obtaining fresh source code and generating a new kernel after such updates. There is usually a time lag between availability of binary updates and availability of the corresponding source code at the Apple Developer Connection Darwin Projects Directory
URL: http://www.opensource.apple.com/darwinsource/, which complicates the update process if an organization chooses to use a customized kernel. It is theoretically possible that a skilled attacker could somehow exploit this race condition to gain system access, but highly unlikely that this particular system under assessment would present a valuable enough prize to warrant such a targeted attack. In other situations involving information of higher value the practice of building a kernel that will implement a "default deny" rule may be desirable. It also may be possible to change the boot sequence to load ipfw rules

before the network is enabled, but investigation of that possibility is beyond the scope of this exercise.

Were assessment and evaluation objectives met?
The objective of this assessment and evaluation is to provide assurance that the target system is being operated in the most secure manner possible within the constraints of budgetary and operational necessities, and to spotlight any shortcomings. An additional objective is to construct an assessment and evaluation checklist that will be usable as a starting point for future evaluations of other systems.

These objectives were both met in the course of creating this report.

REFERENCES:

1. United States Government National Security Agency
"Infosec Assessment Methodology V2.2"
Course Material Presented by Security Horizon, Inc.
Course Workbook

2. United States Government National Security Agency
Infosec Assessment Training and Rating Program
"IAM Home Page"
URL: http://www.iatrp.com/iam.cfm

3. Miles, Greg; Rogers, Russ Et Al.
"Security Assessment: Case Studies for Implementing the NSA-IAM".
Rockland, Mass. Syngress Publishing, Inc. 2004

4. 4 Reference.net
"Mac OS X History"
URL: http://www.4reference.net/encyclopedias/wikipedia/Mac_OS_X_history.html

5. Schwartau, Winn.
"Time Based Security"
Interpact/Network Associates Special Edition 2nd printing May, 2001

6. Ray, John and William C.
"Mac OS X Maximum Security "
Indianapolis Indiana. Sams Publishing 2003

7. NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION
INFORMATION SYSTEMS SECURITY OFFICE
"Risk Assessment/Countermeasure Analysis/Security Test and Evaluation
(ST&E) for Mac OS X (Version 10.1 or later) Computer Systems"
Version 1.0 January 3, 2002
URL: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_macOSX.html

8. Lagoon Software
MacAnalysis vulnerability evaluation tool V.2.3X
URL: http://www.macanalysis.com/about.php3

9. The SANS Top 20 Vulnerabilities
URL: http://www.sans.org/top20/

10. SANS Institute. Track 7
Auditing Networks, Perimeters and Systems
7.6 Advanced System Audit: UNIX workbook

11. Leon Towns-von Stauber
"Security"
Occam's Razor Mac OS X Presentations:
Copyright © 1999-2004 Occam's Razor. All rights reserved.
URL: http://www.occam.com/ocr/osx/

12. Chris Cochella
"Configuring Jaguar's Firewall"
O' Reilly MacDevCenter.com
12/27/2002
URL: http://www.macdevcenter.com/pub/a/mac/2002/12/27/macosx_firewall.html

13. SANS Institute Track 7
Auditing Networks, Perimeters and Systems
7.2 "Auditing the Perimeter":

14. SANS Institute. Track 7
Auditing Networks, Perimeters and Systems
7.6 Advanced System Audit: "Network Auditing Essentials"

15. Robertson, Craig,
"Securing GIAC Enterprises FreeBSD as a Firewall Platform"
GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.8
SANS InfoSec Reading Room. 6 January 2003
URL: http://www.giac.org/practical/GCFW/Craig_Robertson_GCFW.pdf

16. Nawyn, Kenneth E.
"A Security Analysis of System Event Logging with Syslog"
SANS InfoSec Reading Room, June 27, 2003.
URL: http://www.sans.org/rr/papers/index.php?id=1101

17. Marius Schamschula
"How to Configure logcheck Under Mac OS X"
Version 1.2.5 - 20021124
© The Huntsville Macintosh Users Group 2001, 2002
URL: http://www.hmug.org/HowTos/logcheck.html

18. Trevor Warren
"Intrusion Detection Systems, Part IV: Logcheck"
Posted: (2001-02-12 11:26:06 EST)
URL: http://www.freeos.com/articles/3540/

19. United States Government National Security Agency
Infosec Assessment Training and Rating Program
"IAM 18 Baseline INFOSEC Categories"
URL: http://www.iatrp.com/iam18baseline.cfm

20. Little Snitch Application Supervisor
Objective Development
Copyright © 2004 Objective Development
URL: http://www.obdev.at/products/littlesnitch/index.html

21. "OpenSSH features"
URL: http://openssh.com/features.html - Port Forwarding

22. SSH Communications Security
"Secure Shell version 1 vulnerabilities reported by CERT"
SSH Company News Room
© 2002 SSH Communications Security Corp.
URL: http://www.ssh.com/company/newsroom/article/212/

23. Spam Assassin
"Welcome to SpamAssassin"
URL: http://www.spamassassin.org/index.html

24. PGP Corporation
"PGP Personal Desktop"
© 2004 PGP Corporation. All rights reserved.
URL: http://www.pgp.com/products/personal/features.html

25. Al Fasoldt
technofile
"Mac OS X computers don't need antivirus software,
but users should avoid forwarding suspicious mail"
Copyright © 2003, Al Fasoldt Copyright © 2003, The Post-Standard
URL: http://aroundcny.com/technofile/texts/mac070203.html

26. Online Eicar
"Anti-Virus test file"
1 May 2003
© 1998-2004 by eicar e.V
URL: http://www.eicar.org/anti_virus_test_file.htm

27. Tripwire Inc.
"Change Monitoring and Reporting Systems"
© 2004 Tripwire, Inc
URL: http://www.tripwire.com/products/index.cfm

28. Jim Dalrymple
"Mac OS X Software Update security issue uncovered"
MacCentral
July 08, 2002 9:05 pm
Copyright © 2003 Mac Publishing LLC. All rights reserved
URL:
http://maccentral.macworld.com/news/2002/07/08/update/index.php?redirect=1081111615000

29. Gordon Davisson
"Mac OS X: What Are All Those Processes?
A short list of background processes and daemons"
Westwind Computing
Copyright (c) 2002-2003, Westwind Computing inc.
URL: http://www.westwind.com/reference/OS-X/background-processes.html

30. "What is Anacron?"
URL: http://anacron.sourceforge.net/

31. Carnegie-Mellon University Software Engineering Group
CERT Coordination Center
"UNIX Security Checklist v2.0
2.0 Network Services"
URL: http://www.cert.org/tech_tips/usc20_full.html - 2.0

32. CodeSamurai of SecureMac.com
"Open Firmware Password Protection"
SecureMac.com
(c) 2002 SecureMac.com and respected owners
URL: http://www.securemac.com/openfirmwarepasswordprotection.php

33. Fyodor <fyodor@insecure.org>
"The Art of Port Scanning"
Insecure.org
(Last significant update: Sat Sep 6 03:24:53 GMT 1997)
URL: http://www.insecure.org/nmap/nmap_doc.html

34. Spychecker.com
"What is Spyware?"
URL: http://www.spychecker.com/spyware.html

35. Ethereal.com
"Introduction"
URL: http://www.ethereal.com/introduction.html

36. United States Government Department of Energy
Computer Incident Advisory Capability (CIAC)
CIACTech02-003: "Protecting Office for Mac X Antipiracy Server Ports"
April 26, 2002 00:00 GMT
Revised: 7 May 2002
URL: http://www.ciac.org/ciac/techbull/CIACTech02-003.shtml

37. SereneScreen.com
"SereneScreen Marine Aquarium 2 - Mac OS X"
URL: http://www.serenescreen.com/product/maquariumx/

38. mutt.org
"The Mutt E-Mail Client"
URL: http://www.mutt.org/

39. Bombich Software
"Carbon Copy Cloner"
Copyright 2002-2004 Mike Bombich
URL: http://www.bombich.com/software/ccc.html

40. Roxio, Inc
"Roxio Toast Titanium"
© 2004 Roxio, Inc. All Rights Reserved.
URL: http://www.roxio.com/en/products/toast/index.jhtml

41. Kensington Technology Group
"MicroSaver Security Cable"
©2004 Kensington Technology Group,
URL: http://www.kensington.com/html/2219.html

42. Apple Developer Connection
Darwin Projects Directory (requires free account for access)
URL: http://www.opensource.apple.com/darwinsource/

Appendices

Appendix 1: Internet Daemon Configuration Files:

```
cat /etc/inetd.conf
# WARNING
#
# Mac OS 10.2 and forward uses xinetd instead of the traditional inetd.
# See xinetd.conf(5) if you need to add a service to run out of xinetd.
# Please use /sbin/service to interface over editing the shipped files
# in /etc/xinetd.d directly. For example:
# /sbin/service telnet start
# /sbin/service telnet stop
# /sbin/service --list
#
# Internet server configuration database
#
#       @(#)inetd.conf  5.4 (Berkeley) 6/30/90
#
# Items with double hashes in front (##) are not yet implemented in the OS.
#
#finger stream  tcp     nowait  nobody  /usr/libexec/tcpd             fingerd -s
#ftp    stream  tcp     nowait  root    /usr/libexec/tcpd             ftpd -l
#login  stream  tcp     nowait  root    /usr/libexec/tcpd             rlogind
#nntp   stream  tcp     nowait  usenet  /usr/libexec/tcpd             nntpd
#ntalk  dgram   udp     wait    root    /usr/libexec/tcpd             ntalkd
#shell  stream  tcp     nowait  root    /usr/libexec/tcpd             rshd
#telnet stream  tcp     nowait  root    /usr/libexec/tcpd             telnetd
#uucpd  stream  tcp     nowait  root    /usr/libexec/tcpd             uucpd
#comsat dgram   udp     wait    root    /usr/libexec/tcpd             comsat
#tftp   dgram   udp     wait    nobody  /usr/libexec/tcpd             tftpd
/private/tftpboot
#bootps dgram   udp     wait    root    /usr/libexec/tcpd             bootpd
##pop3  stream  tcp     nowait  root    /usr/libexec/tcpd     /usr/local/libexec/popper
#pop3   stream  tcp nowait  root  /usr/libexec/tcpd /usr/libexec/popper qpopper -s
##imap4 stream  tcp     nowait  root    /usr/libexec/tcpd   /usr/local/libexec/imapd
#
# "Small servers" -- used to be standard on, but we're more conservative
# about things due to Internet security concerns.  Only turn on what you
# need.
#
#chargen stream tcp     nowait  root    internal
#chargen dgram  udp     wait    root    internal
#daytime stream tcp     nowait  root    internal
#daytime dgram  udp     wait    root    internal
#discard stream tcp     nowait  root    internal
#discard dgram  udp     wait    root    internal
#echo    stream tcp     nowait  root    internal
#echo    dgram  udp     wait    root    internal
```

```
#time    stream tcp     nowait  root    internal
#time    dgram  udp     wait    root    internal
#
# Kerberos (version 5) authenticated services
#
##eklogin  stream tcp   nowait root     /usr/libexec/tcpd       klogind -k -c -e
##klogin   stream tcp   nowait root     /usr/libexec/tcpd       klogind -k -c
##kshd     stream tcp   nowait root     /usr/libexec/tcpd       kshd -k -c -A
#krb5_prop stream tcp   nowait root     /usr/libexec/tcpd       kpropd
#
# RPC based services (you MUST have portmapper running to use these)
#
##rstatd/1-3    dgram rpc/udp wait root /usr/libexec/tcpd       rpc.rstatd
##rusersd/1-2   dgram rpc/udp wait root /usr/libexec/tcpd       rpc.rusersd
##walld/1       dgram rpc/udp wait root /usr/libexec/tcpd       rpc.rwalld
##pcnfsd/1-2    dgram rpc/udp wait root /usr/libexec/tcpd       rpc.pcnfsd
##rquotad/1     dgram rpc/udp wait root /usr/libexec/tcpd       rpc.rquotad
##sprayd/1      dgram rpc/udp wait root /usr/libexec/tcpd       rpc.sprayd
#
# The following are not known to be useful, and should not be enabled unless
# you have a specific need for it and are aware of the possible implications.
#
#exec   stream  tcp     nowait  root    /usr/libexec/tcpd       rexecd
#auth   stream  tcp     wait    root    /usr/libexec/identd     identd -w -t120
```

```
ls -al /etc/xinetd.d
total 108
drwxr-xr-x   29 root  wheel   986  5 Feb 13:58 .
drwxr-xr-x  106 root  wheel  3604  4 Mar 19:35 ..
-rw-r--r--    1 root  wheel   143 12 Sep 21:44 auth
-rw-r--r--    1 root  wheel   145 12 Sep 21:44 bootps
-rw-r--r--    1 root  wheel   155 12 Sep 21:44 chargen
-rw-r--r--    1 root  wheel   158 12 Sep 21:44 chargen-udp
-rw-r--r--    1 root  wheel   145 12 Sep 21:44 comsat
-rw-r--r--    1 root  wheel   155 12 Sep 21:44 daytime
-rw-r--r--    1 root  wheel   158 12 Sep 21:44 daytime-udp
-rw-r--r--    1 root  wheel   149 12 Sep 21:44 echo
-rw-r--r--    1 root  wheel   152 12 Sep 21:44 echo-udp
-rw-r--r--    1 root  wheel   315 19 Sep 17:50 eppc
-rw-r--r--    1 root  wheel   143 12 Sep 21:44 exec
-rw-r--r--    1 root  wheel   166 12 Sep 21:44 finger
-rw-r--r--    1 root  wheel   163 12 Sep 21:44 ftp
-rw-r--r--    1 root  wheel   145 12 Sep 21:44 login
-r--r--r--    1 root  wheel   198 19 Sep 02:13 nmbd
-rw-r--r--    1 root  wheel   144 12 Sep 21:44 ntalk
-rw-r--r--    1 root  wheel   230 19 Sep 23:53 printer
-rw-r--r--    1 root  wheel   281  5 Feb 13:57 qpopper
-rw-r--r--    1 root  wheel   142 12 Sep 21:44 shell
```

```
-r--r--r--    1 root  wheel   247 19 Sep 02:13 smb-direct
-r--r--r--    1 root  wheel   199 19 Sep 02:13 smbd
-r--r--r--    1 root  wheel   208 25 Sep 16:11 ssh
-r--r--r--    1 root  wheel   179 19 Sep 02:13 swat
-rw-r--r--    1 root  wheel   146 12 Sep 21:44 telnet
-rw-r--r--    1 root  wheel   191 12 Sep 21:44 tftp
-rw-r--r--    1 root  wheel   149 12 Sep 21:44 time
-rw-r--r--    1 root  wheel   152 12 Sep 21:44 time-udp
```

cat /etc/xinetd.d/auth

cat /etc/xinetd.d/qpopper (Note: Disabled services not included)

```
service pop3
{
        disable         = no
        socket_type     = stream
        wait            = no
        user            = root
        protocol        = tcp
        bind            = 127.0.0.1
        groups          = yes
        server          = /usr/libexec/popper
}
```

Appendix 2: Process Listing

Identify active processes.

Run "ps axuc" in shell window

Some fields not relevant to the exercise have been deleted to enhance formatting

```
USER       PID %CPU %MEM    VSZ    RSS    TIME COMMAND
root         1    0    0  18072    304 00:00.0 init
root         2    0    0  18604    204 00:00.1 mach_init
root        81    0    0  18092    196 00:00.1 syslogd
root        87    0  0.1  27868   1244 00:01.6 kextd
root        89    0  0.2  29824   1892 00:01.3 configd
root        90    0  0.1  27880    924 00:00.3 diskarbitrationd
root        92    0    0  18676    260 00:00.1 notifyd
root        94    0    0  27480    372 00:00.4 netinfod
root        96    0    0  18056    120 00:01.8 update
root        99    0    0  18080    124 00:00.0 dynamic_pager
root       129    0  0.6  34808   6096 00:00.9 coreservicesd
root       131    0  0.1  27752    684 00:00.1 distnoted
nobody     143    0  0.1  27968    804 00:00.1 mDNSResponder
root       144    0    0  27340    128 00:00.0 KernelEventAgent
root       145    0    0  27612    152 00:00.1 cron
root       156    0  0.1  29548   1184 00:00.1 SecurityServer
claudel    162  0.1    4 219676  41640 01:19.1 WindowServer
claudel    180    0  0.4  75912   4648 00:01.9 ATSServer
claudel    188    0  0.5 138064   4772 00:00.8 loginwindow
root       189    0    0  18320    292 00:01.0 ntpd
root       202    0  0.2  31352   2416 00:00.6 DirectoryService
root       218    0  0.1  29176   1300 00:07.0 lookupd
root       243    0    0  27332    172 00:00.0 crashreporterd
root       271    0  0.1  29016   1572 00:01.2 cupsd
root       276    0    0  27484    300 00:00.0 xinetd
root       281    0  0.1  18776    604 00:00.7 httpd
www        285    0    0  18772    228 00:00.0 httpd
root       337    0  0.1  27476    696 00:00.1 master
claudel    341    0  0.2  45316   1588 00:00.2 pbs
claudel    346    0  0.3 154992   3496 00:01.6 Dock
claudel    347    0  0.5 149648   4820 00:03.4 SystemUIServer
claudel    348    0    1 163052  10876 00:03.2 Finder
claudel    354    0  0.5 150096   5332 00:01.6 LittleSnitchDaemon
claudel    356    0  0.3  74992   2640 00:10.5 PGPdiskEngine
claudel    368  6.1  1.3 165456  13252 00:41.8 Terminal
```

```
root       380     0     0   27540    488  00:00.0 login
claudel    392     0   2.3  183004  23924  00:38.9 Safari
claudel    394     0     0   18192    304  00:00.0 tail
postfix    426     0   0.1   27556    772  00:00.1 qmgr
root       435     0     0   27540    500  00:00.0 login
claudel    446     0   0.1   27548    844  00:00.5 ssh
claudel    526  77.8   3.7  222808  39308  19:06.0 Microsoft Word
claudel    527     0   0.4  142104   4520  00:00.7 Microsoft Database Daemon
root       540     0     0   27540    500  00:00.0 login
claudel    585     0   0.5  152024   5212  00:01.2 SecurityAgent
root       600     0     0   18108    356  00:00.0 ps
```

Appendix 3: Active Internet Connections and Domain Sockets

Run "netstat -a" in shell window

Include output in report

Active Internet connections (including servers)

```
Proto  Recv-Q  Send-Q         Local Address     Foreign Address          (state)
 tcp4       0       0                *.3942                 *.*           LISTEN
 tcp4       0       0       localhost.10025                 *.*           LISTEN
 tcp6       0       0       localhost.10025                 *.*           LISTEN
 tcp4       0       0       localhost.10110                 *.*           LISTEN
 tcp6       0       0       localhost.10110                 *.*           LISTEN
 tcp4       0       0         x.x.x.x.49398         isp.net.ssh      ESTABLISHED
 tcp4       0       0         localhost.ipp                 *.*           LISTEN
 tcp4       0       0                *.pop3                 *.*           LISTEN
 tcp4       0       0                *.http                 *.*           LISTEN
 tcp4       0       0               *.https                 *.*           LISTEN
 tcp4       0       0     localhost.netinfo-          localhost      ESTABLISHED
                                      local
 tcp4       0       0         localhost.954  localhost.netinfo-      ESTABLISHED
                                                          local
 tcp4       0       0     localhost.netinfo-                *.*           LISTEN
                                      local
 udp4       0       0      *.rockwell-csp2                  *.*
 udp4       0       0                 *.ipp                 *.*
 udp4       0       0                *.mdns                 *.*
 udp4       0       0           z.z.z.z.ntp                 *.*
 udp4       0       0         localhost.ntp                 *.*
 udp4       0       0                 *.ntp                 *.*
 udp4       0       0              *.bootpc                 *.*
 udp4       0       0     localhost.netinfo-                *.*
                                      local
 udp4       0       0              *.syslog                 *.*
 udp6       0       0                 *.514                 *.*
 icm6       0       0                   *.*                 *.*
```

Active LOCAL (UNIX) domain sockets

```
Address Type    Recv-Q  Send-Q     Inode      Conn   Refs  Nextref Addr
 2865850 stream      0       0         0   2865818      0        0
 2865818 stream      0       0         0   2865850      0        0
 28657a8 stream      0       0         0   2865888      0        0
 2865888 stream      0       0         0   28657a8      0        0
 2865968 stream      0       0         0   2865578      0        0
 2865578 stream      0       0         0   2865968      0        0
2.87E+04 stream      0       0         0         0      0        0 /tmp/.pgpdisk-claudel-501-sock
 28658c0 stream      0       0  29a4690          0      0        0 /tmp/.pgpdisk-claudel-501-sock
 2865a10 stream      0       0         0   2865a48      0        0 /var/run/pppconfd
 2865a48 stream   0   0        0  2865a10   0   0
 2865a80 stream   0   0        0  2865ab8   0   0 /var/run/pppconfd
 2865ab8 stream   0   0        0  2865a80   0   0
 2865af0 stream   0   0        0  2865b28   0   0
 2865b28 stream   0   0        0  2865af0   0   0
 2865b60 stream   0   0        0  2865b98   0   0
 2865b98 stream 100   0        0  2865b60   0   0
 2865bd0 stream   0   0        0  2865c08   0   0
 2865c08 stream   0   0        0  2865bd0   0   0
 2865c40 stream   0   0        0  2865c78   0   0
 2865c78 stream   0   0        0  2865c40   0   0
 2865cb0 stream   0   0  2839be8        0   0   0 private/bsmtp
 2865ce8 stream   0   0        0  2865d20   0   0
 2865d20 stream   0   0        0  2865ce8   0   0
 2865d58 stream   0   0  2839c80        0   0   0 private/ifmail
 2865d90 stream   0   0        0  2865dc8   0   0
 2865dc8 stream   0   0        0  2865d90   0   0
2.87E+03 stream   0   0  2839d18        0   0   0 private/uucp
2.87E+41 stream   0   0        0 2.87E+73   0   0
2.87E+73 stream   0   0        0 2.87E+41   0   0
 2865ea8 stream   0   0  2839db0        0   0   0 private/cyrus
 2865ee0 stream   0   0        0  2865f18   0   0
 2865f18 stream   0   0        0  2865ee0   0   0
 2865f50 stream   0   0 2.84E+51        0   0   0 private/old-cyrus
 2865f88 stream   0   0        0  2865fc0   0   0
 2865fc0 stream   0   0        0  2865f88   0   0
 1b22000 stream   0   0  2839ee0        0   0   0 private/maildrop
 1b22038 stream   0   0        0  1b22070   0   0
 1b22070 stream   0   0        0  1b22038   0   0
 1b220a8 stream   0   0  2839f78        0   0   0 private/lmtp
 1b220e0 stream   0   0        0  1b22118   0   0
 1b22118 stream   0   0        0  1b220e0   0   0
 1b22150 stream   0   0  283a010        0   0   0 private/virtual
 1b22188 stream   0   0        0  1b221c0   0   0
 1b221c0 stream   0   0        0  1b22188   0   0
 1b221f8 stream   0   0  283a0a8        0   0   0 private/local
 1b22230 stream   0   0        0  1b22268   0   0
 1b22268 stream   0   0        0  1b22230   0   0
 1b222a0 stream   0   0  283a140        0   0   0 private/error
 1b222d8 stream   0   0        0  1b22310   0   0
 1b22310 stream   0   0        0  1b222d8   0   0
 1b22348 stream   0   0  283a1d8        0   0   0 public/showq
```

```
1b22380 stream    0    0        0  1b223b8        0        0
1b223b8 stream    0    0        0  1b22380        0        0
1b223f0 stream    0    0  283a270        0        0        0 private/relay
1b22428 stream    0    0        0  1b22460        0        0
1b22460 stream    0    0        0  1b22428        0        0
1b22498 stream    0    0  283a308        0        0        0 private/smtp
1b224d0 stream    0    0        0  1b22508        0        0
1b22508 stream    0    0        0  1b224d0        0        0
1b22540 stream    0    0  283a3a0        0        0        0 private/proxymap
1b22578 stream    0    0        0  1b225b0        0        0
1b225b0 stream    0    0        0  1b22578        0        0
1b225e8 stream    0    0  283a438        0        0        0 public/flush
1b22620 stream    0    0        0  1b22658        0        0
1b22658 stream    0    0        0  1b22620        0        0
1b22690 stream    0    0  283a4d0        0        0        0 private/defer
1b226c8 stream    0    0        0  1b22700        0        0
1b22700 stream    0    0        0  1b226c8        0        0
1b22738 stream    0    0  283a568        0        0        0 private/bounce
1b22770 stream    0    0        0  1b227a8        0        0
1b227a8 stream    0    0        0  1b22770        0        0
1b227e0 stream    0    0  283a600        0        0        0 private/rewrite
1b22818 stream    0    0        0  1b228c0        0        0
1b228c0 stream    0    0        0  1b22818        0        0
1b22850 stream    0    0        0  1b228f8        0        0
1b228f8 stream    0    0        0  1b22850        0        0
1b229d8 stream    0    0        0  1b22968        0        0
1b22968 stream    0    0        0  1b229d8        0        0
1b22af0 stream    0    0  283a730        0        0        0 public/cleanup
1b22a10 stream    0    0        0  1b229a0        0        0
1b229a0 stream    0    0        0  1b22a10        0        0
1b22a80 stream    0    0        0  1b22b98        0        0
1b22b98 stream    0    0        0  1b22a80        0        0
1b22888 stream    0    0        0  1b22ab8        0        0
1b22ab8 stream    0    0        0  1b22888        0        0
1b22d20 stream    0    0  2119730        0        0        0 /var/run/pppconfd
1b22e38 stream    0    0  20ed018        0        0        0 /var/run/mDNSResponder
2865658 dgram     0    0        0  1b22fc0        0   3E+06
2865930 dgram     0    0        0  1b22fc0        0  28658f8
28658f8 dgram     0    0        0  1b22fc0        0  1b22930
28659a0 dgram     0    0        0  28659d8  28659d8        0
28659d8 dgram     0    0        0  28659a0  28659a0        0
1b22930 dgram     0    0        0  1b22fc0        0  1b22a48
```

```
1b22a48 dgram    0    0       0  1b22fc0        0 1b22b28
1b22b28 dgram    0    0       0  1b22fc0        0 1b22b60
1b22b60 dgram    0    0       0  1b22fc0        0 1b22e70
1b22e70 dgram    0    0       0  1b22fc0        0 1b22bd0
1b22bd0 dgram    0    0       0  1b22fc0        0 1b22cb0
1b22cb0 dgram    0    0       0  1b22fc0        0 1b22d58
1b22d58 dgram    0    0       0  1b22fc0        0 1b22d90
1b22d90 dgram    0    0       0  1b22fc0        0 1b22c78
1b22c78 dgram    0    0       0  1b22fc0        0 1b22e00
1b22dc8 dgram    0    0       0 1b22ce8 1b22ce8         0
1b22ce8 dgram    0    0       0 1b22dc8 1b22dc8         0
1b22e00 dgram    0    0       0  1b22fc0        0 1b22ee0
1b22c08 dgram    0    0       0 1b22c40 1b22c40         0
1b22c40 dgram    0    0       0 1b22c08 1b22c08         0
1b22ee0 dgram    0    0       0  1b22fc0        0 1b22f18
 1b22f18 dgram   0    0       0  1b22fc0        0 1b22f88
 1b22f88 dgram   0    0       0  1b22fc0        0 1b22f50
 1b22f50 dgram   0    0       0  1b22fc0        0         0
 1b22fc0 dgram   0    0 1b61268        0  ####            0 /var/run/syslog
```

Appendix 4: Nessus Scan Results

Internal scan

```
Nessus Scan Report
------------------
SUMMARY
 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 2
 - Number of security notes found : 6

TESTED HOSTS
 x.x.x.x (Security warnings found)

DETAILS
+ x.x.x.x :
 . List of open ports :
   o pop3 (110/tcp) (Security notes found)
   o nessus (1241/tcp) (Security warnings found)
   o unknown (3869/tcp)
   o X11 (6000/tcp) (Security warnings found)
   o bootpc (68/udp)
   o ntp (123/udp)
   o netbios-ns (137/udp)
   o netbios-dgm (138/udp)
   o netbios-ssn (139/udp)
   o syslog (514/udp)
   o general/tcp (Security notes found)

 . Information found on port pop3 (110/tcp
    The service closed the connection after 0 seconds without sending any data
    It might be protected by some TCP wrapper


 . Warning found on port nessus (1241/tcp)
    A Nessus Daemon is listening on this port.
 . Information found on port nessus (1241/tcp)
    A TLSv1 server answered on this port

 . Information found on port nessus (1241/tcp)
    Here is the TLSv1 server certificate:
    Certificate:
        Data:
            Version: 3 (0x2)
            Serial Number: 1 (0x1)
            Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, L=Here, O=Nessus Users United, OU=Certification
     Authority for Blossom.local,
CN=Blossom.local/emailAddress=ca@Blossom.local
        Validity
            Not Before: Nov 13 20:33:44 2003 GMT
            Not After : Nov 12 20:33:44 2004 GMT
        Subject: C=US, L=Here, O=Nessus Users United, OU=Server certificate
     for Blossom.local, CN=Blossom.local/emailAddress=nessusd@Blossom.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d6:d5:e5:e8:e4:c4:6f:40:23:7d:35:2e:52:5f:
                    47:df:10:19:2e:3c:c4:51:85:63:4d:39:bb:79:08:
                    4b:96:57:89:cd:8f:69:c8:47:27:1b:04:df:84:17:
                    98:d7:40:01:80:63:67:1d:a1:61:4d:99:82:41:27:
                    57:a4:eb:3c:eb:7e:bf:90:36:f4:71:84:1b:8a:50:
                    6b:4b:6a:de:af:6f:b0:a2:ad:e1:9c:8d:3d:76:ee:
                    70:b2:b8:83:53:9a:e8:86:50:2c:8b:d1:4c:db:80:
                    ec:29:f4:58:43:c1:87:8f:ac:73:90:c5:6b:fa:4f:
                    fc:50:e3:0a:ae:94:ee:0a:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                SSL Server
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                34:C0:D1:DF:27:20:26:BF:94:0E:EB:D5:1D:EA:16:35:03:21:C6:CD
            X509v3 Authority Key Identifier:

     keyid:EA:79:53:2C:E3:D7:AD:95:2B:CC:5D:B5:E3:01:1F:58:00:4E:50:09
                DirName:/C=US/L=Here/O=Nessus Users United/OU=Certification
     Authority for
Blossom.local/CN=Blossom.local/emailAddress=ca@Blossom.local
                serial:00

            X509v3 Subject Alternative Name:
                email:nessusd@Blossom.local
            X509v3 Issuer Alternative Name:
                <EMPTY>

    Signature Algorithm: md5WithRSAEncryption
        87:13:a5:0d:a5:40:13:2b:bf:e9:59:34:05:c2:98:4f:d0:58:
        56:74:70:54:84:3a:e5:a4:a1:d4:9e:d3:e8:f3:f2:b4:08:29:
        6c:d8:2f:ec:20:38:77:98:7f:ef:7c:9e:7f:e3:0a:94:01:43:
            a3:e9:36:31:3c:cf:02:99:d6:bb:50:8a:ff:41:2b:83:0e:3d:
            c6:6c:0d:35:c3:b1:7a:ed:4f:51:3d:eb:2c:d2:66:e5:75:94:
            1c:aa:85:89:fc:01:e4:7b:d1:1b:ed:6a:a5:d6:74:8c:38:4e:
            29:b2:ab:e2:25:93:19:29:fc:16:1c:08:0c:81:44:1b:3d:c1:
            5d:eb

 . Information found on port nessus (1241/tcp)
   This TLSv1 server does not accept SSLv2 connections.
   This TLSv1 server does not accept SSLv3 connections.

 . Warning found on port X11 (6000/tcp)
   This X server does *not* allow any client to connect to it
   however it is recommended that you filter incoming connections
   to this port as attacker may send garbage data and slow down
   your X session or even kill the server.

   Here is the server version : 11.0
   Here is the message we received : No protocol specified


   Solution : filter incoming connections to ports 6000-6009
   Risk factor : Low
   CVE : CVE-1999-0526

 . Information found on port general/tcp
   Nmap found that this host is running Apple Mac OX X 10.3.0 - 10.3.2
    (Panther)

 . Information found on port general/tcp
   HTTP NIDS evasion functions are enabled.
   You may get some false negative results
------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Internal scan with firewall disabled for comparison

```
Nessus Scan Report
------------------
SUMMARY
 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 2
 - Number of security notes found : 11

TESTED HOSTS
 blossom.local (Security warnings found)
```

```
DETAILS
+ blossom.local :
 . List of open ports :
   o http (80/tcp) (Security notes found)
   o pop3 (110/tcp) (Security notes found)
   o nessus (1241/tcp) (Security warnings found)
   o unknown (3869/tcp)
   o X11 (6000/tcp) (Security warnings found)
   o bootpc (68/udp)
   o syslog (514/udp)
   o general/tcp (Security notes found)

 . Information found on port http (80/tcp)
    A web server is running on this port

 . Information found on port http (80/tcp)
    Nessus was not able to reliably identify this server. It might be:
    Apache/1.3.27 (Unix)  (Red-Hat/Linux) mod_jk/1.2.4 mod_ssl/2.8.12
     OpenSSL/0.9.6b PHP/4.1.2 mod_perl/1.26
    The fingerprint differs from these known signatures on 7 point(s)

 . Information found on port http (80/tcp)
    The remote web server type is :
        Apache/1.3.29 (Darwin)

    Solution : You can set the directive 'ServerTokens Prod' to limit
    the information emanating from the server in its response headers.

 . Information found on port pop3 (110/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

 . Warning found on port nessus (1241/tcp)
    A Nessus Daemon is listening on this port.

 . Information found on port nessus (1241/tcp)
    A TLSv1 server answered on this port
 . Information found on port nessus (1241/tcp)
    Here is the TLSv1 server certificate:
< Certificate Information deleted >:

 . Information found on port nessus (1241/tcp)
    This TLSv1 server does not accept SSLv2 connections.
    This TLSv1 server does not accept SSLv3 connections.


 . Warning found on port X11 (6000/tcp)
This X server does *not* allow any client to connect to it
```

```
however it is recommended that you filter incoming connections
to this port as attacker may send garbage data and slow down
your X session or even kill the server.

Here is the server version : 11.0
Here is the message we received : No protocol specified

    Solution : filter incoming connections to ports 6000-6009
    Risk factor : Low
    CVE : CVE-1999-0526

 . Information found on port general/tcp
    Nmap found that this host is running Apple Mac OX X 10.3.0 - 10.3.2
     (Panther)

 . Information found on port general/tcp
    HTTP NIDS evasion functions are enabled.
    You may get some false negative results

 . Information found on port general/tcp
    x.x.x.x resolves as blossom.local.

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Scan from external machine

```
Nessus Scan Report
------------------
SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 0
 - Number of security notes found : 2

TESTED HOSTS
 x.x.x.x (Security notes found)

DETAILS

+ x.x.x.x :
 . List of open ports :
   o general/tcp (Security notes found)

 . Information found on port general/tcp
    The remote host is up
 . Information found on port general/tcp
    HTTP NIDS evasion functions are enabled.
    You may get some false negative results

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Scan from external machine with firewall disabled for comparison, and to simulate firewall breakdown or penetration.

```
Nessus Scan Report
------------------
SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 1
 - Number of security notes found : 7

TESTED HOSTS
 x.x.x.x (Security warnings found)

DETAILS
+ x.x.x.x :
 . List of open ports :
   o general/tcp (Security notes found)
   o bootpc (68/udp)
   o http (80/tcp) (Security warnings found)
   o pop3 (110/tcp) (Security notes found)
   o syslog (514/udp)
   o general/udp (Security notes found)

 . Information found on port general/tcp
    The remote host is up

 . Information found on port general/tcp
    HTTP NIDS evasion functions are enabled.
    You may get some false negative results

 . Information found on port general/tcp
    The remote host is running MacOS X 10.3

 . Warning found on port http (80/tcp)

    It seems that your web server tries to hide its version
    or name, which is a good thing.
    However, using a special crafted request, Nessus was able
    to determine that is running :
     Apache/1.3.29 (Darwin)

    Risk factor : None
    Solution : Fix your configuration.

 . Information found on port http (80/tcp)
    A web server is running on this port
. Information found on port http (80/tcp)
    Nessus was not able to reliably identify this server. It might be:
    Apache/1.3.27 (Unix)  (Red-Hat/Linux) mod_jk/1.2.4 mod_ssl/2.8.12
     OpenSSL/0.9.6b PHP/4.1.2 mod_perl/1.26
    The fingerprint differs from these known signatures on 7 point(s)

 . Information found on port pop3 (110/tcp)
    The service closed the connection after 0 seconds without sending any data
    It might be protected by some TCP wrapper

 . Information found on port general/udp
    For your information, here is the traceroute to x.x.x.x :
    y.y.y.y
    x.x.x.x

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```