



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gsna>

Audit! Mac OS X ‘Panther’ on an Apple PowerBook

GSNA Practical Assignment
Version 3.1, Option #1

James Fung

Abstract

A leading research facility (for the purposes of this exercise we'll refer to them as 'GIAC Research Laboratory') is preparing a new rollout of standard laptops for their scientists. Having settled upon the Apple PowerBook and Mac OS X as the platform of choice, the next step is to assess the risks of deploying systems with an out-of-the-box installation of OS X. This document starts with research into the current state of practice involving this particular hardware/software combination. Next, we will develop an audit checklist and perform an actual audit of the system. Finally, we will present a summary report plus some recommendations to address our findings.

© SANS Institute 2004, Author retains full rights

Table of Contents

Part #1 - Research in Audit, Measurement Practice, and Control	4
1.1 - The Subject	4
1.2 - The Risks	4
1.3 - The References	9
Part #2 - Create an Audit Checklist	10
2.1 - The Checklist	10
2.1.1 - Login Banner	10
2.1.2 - Disable Auto-Login	11
2.1.3 - Disable Listing of Usernames in Login Window	11
2.1.4 - Password Protected Screensaver	12
2.1.5 - Screensaver Activation Time	13
2.1.6 - Disable Root Account	14
2.1.7 - Use a Non-Privileged Account	15
2.1.8 - Remove Un-Necessary Accounts	16
2.1.9 - Use of Strong Passwords	16
2.1.10 - Home Folder Encryption	17
2.1.11 - Install Anti-Virus Software	18
2.1.12 - Software Update Frequency	19
2.1.13 - Patch, Patch, Patch!	20
2.1.14 - Central System Logs (syslog)	20
2.1.15 - TCP Wrappers	21
2.1.16 - Disable Un-Necessary Network Services	23
2.1.17 - Enable the Firewall	23
2.1.18 - Bluetooth Discovery and Authentication	24
2.1.19 - WiFi Automatic Discovery and Association	25
2.1.20 - Backups	26
2.1.21 - Open Firmware Password	27
Part #3 - Conduct the Audit Testing, Evidence and Findings	28
3.1 - The Audit	28
3.1.1 - Test #1 : Install Anti-Virus Software	28
3.1.2 - Test #2 : Disable Un-Necessary Network Services	29
3.1.3 - Test #3 : Patch, Patch, Patch!	31
3.1.4 - Test #4 : Disable Auto-Login	32
3.1.5 - Test #5 : Home Folder Encryption	33
3.1.6 - Test #6 : Use of Strong Passwords	34
3.1.7 - Test #7 : Enable the Firewall	36
3.1.8 - Test #8 : Open Firmware Password	37
3.1.9 - Test #9 : TCP Wrappers	39
3.1.10 - Test #10 : Central System Logs (syslog)	40
Part #4 - Audit Report or Risk Assessment	42
4.1 - The Summary	42
4.2 - The Findings	43
4.3 - The Recommendations	47
References	50

1.1 – The Subject

The main focus of this audit will be an Apple PowerBook, running Mac OS X (“Panther”). For those unfamiliar with Apple’s product offerings, it is enough to know that the PowerBook is a laptop/notebook computer, fairly light and very portable. For the purpose of this audit the target system is configured as follows:

- 17-inch Apple PowerBook
- Processor: 1GHz PowerPC G4
- Memory: 1GB DDR SDRAM
- Video: nVidia GeForce 4 MX (64 MB)
- Network: Built-in 10/100/1000 Ethernet
- Wireless: Built-in Bluetooth, AirPort Extreme (802.11g)
- Storage: Fujitsu MHS2060AT 60GB IDE HD
- Optical: Matsushita DVD-R UJ-815 DVD-RW/CD-RW
- Modem: Built-in 56kbps V.92 modem
- USB: 2 x USB 1.1 Ports
- Firewire: 1 x Firewire 800 Port, 1 x Firewire 400 Port
- **Operating System: Mac OS X v10.3 (“Panther”)**

This last bullet is likely the most important one. While the specifications can and will differ from system to system, the specific hardware configuration of the laptop will have negligible impact on the outcome of this audit. Why even mention that the system is a laptop then, you ask? Because as we will see later, that the form factor is a laptop means the system will be at more of a risk under certain situations than if we were discussing a desktop workstation or a rack-mount server. The rest of the audit (the bulk of it, actually) will focus on the operating system and its configuration.

This particular system is one of many identical laptops earmarked for scientists at a leading research laboratory. Because some of the research conducted at this facility can be considered sensitive in nature, security will be a top concern. In addition, the Laboratory hosts numerous visiting scientists per year, most of whom will bring their own computers on site. In a situation such as this, the ‘internal’ threat is as serious as the external, since the Laboratory currently has little control over the configuration management of the collaborators’ systems that get brought on-site.

Our goal here is to assess the security of the current configuration of these new Apple notebook computers, and ultimately to develop a secure baseline configuration for these systems such that researchers can do their work without having to worry about their computer system and the data that it holds.

1.2 – The Risks

Before we proceed any further, we will need to first get some definitions out of the

way. We'll be throwing around terminology such as **impact**, **likelihood**, **risk**, **threat**, and **vulnerability**. These definitions are provided here courtesy of the National Institute of Standards and Technology (NIST), specifically Special Publication 800-30.¹

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

- The reader should take note that from a risk management perspective, vulnerabilities do not necessarily have to be technical in nature. A Microsoft Windows 2000 Server running IIS, if left un-patched, certainly has many vulnerabilities that could be exploited over the network. This is what many think of when they hear the word 'vulnerability'. But consider this: the same server, left out in an open area where anybody can sit down at the console without any special permissions. This too is a vulnerability, though of the physical kind.

Threat: The potential for a particular threat-source to successfully exercise (accidentally trigger or intentionally exploit) a particular vulnerability.

- Again, the threat-source in this definition need not be technical in nature. Depending on where you live, a monsoon could well be a threat-source. For others, un-educated system administrators may well pose the biggest threat.

Likelihood: An overall rating that indicates the probability that a potential vulnerability may be exercised.

- This is usually expressed simply with a "High/Medium/Low" ratings scale. Many factors go into assigning a rating, including (but not limited to): the capability of the particular threat-source, the existence (or lack) of countermeasures and safeguards, etc.

Impact: The loss resulting from the successful threat exercise of a vulnerability.

- Sometimes expressed relative to the ever-popular CIA Triad² (Confidentiality, Integrity, Availability), other times expressed in an actual dollar (or your currency of choice) amount. For instance, how much importance does a bank place on its ATM network? What would happen should an Internet worm succeed in disabling the systems that govern the network, making the automated teller machines inaccessible³? Surely a loss in revenue for the duration of the outage, but what about after? A loss in consumer confidence and resulting public relations crisis may very well end up costing the organization more than the actual outage.

Risk, then, is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

¹ <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

² http://www.securitygroup.org/wiki/wiki.php?title=CIA_triad

³ <http://www.cnn.com/2003/TECH/internet/01/26/internet.attack/>

Now that we have the definitions out of the way, it's time to proceed with our audit. First, we start by listing some scenarios involving our test subject (the PowerBook 17) where damage can occur.

Table 1 on the next page is a matrix detailing some of the vulnerabilities, threats, and damage that our system will be faced with. The last column is a risk rating. The final risk rating is derived with the help from the following table, again courtesy of NIST:

Impact \ Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

As can be seen here, a final risk rating is assigned based on the values of the Likelihood multiplied by Impact. A 'Low' risk is a value from 1-10. 'Medium', 11-50. A 'High' risk is awarded for any result greater than 50.

Table 2 describes those areas of the organization most likely to be impacted should something befall these systems. Though we are testing one single system for the purposes of this exercise, it is important to be aware that any potential impact mentioned in this document will be many times greater in actuality, due to the fact that this is but one of many identical systems to be deployed 'out in the field'. One vulnerability identified here may translate to well over a hundred, one for each of the laptops deployed by the Laboratory. Because systems in question are end-user workstations, impact on the actual computing infrastructure of the Laboratory will be minimal. However other major areas will be adversely impacted, as seen on page 8.

Note that throughout this document, Likelihood, Impact, and Risk are all rated on a Low-Medium-High scale. Yes, readers, this is all very subjective! The risk analysis performed here is qualitative in nature, and relies heavily on the experiences and judgments of the individual(s) performing the analysis. The three-point scale was chosen because it was well-suited for the purposes of this audit. It's both granular and simple enough that we'll be able to properly communicate the level of risk to management without complicating matters needlessly. Readers should free to work with whatever point-scale they feel will best communicate their thoughts across. Depending on the subject being audited and the audience involved, a more granular scale may produce more ideal results for the client/organization.

Table 1 – Vulnerabilities, Threats: their capacity to inflict damage and impact on an organization

Vulnerability	Threat	Damage	Source	Likelihood	Impact	Risk
Lack of training	User error		Un-trained Employee	Medium	Medium	Medium
Un-patched or mis-configured OS	Malware (virus, Trojan, etc.)	Loss of Data	- Competitor - “Script Kiddies”	Medium	Medium	Medium
	Directed attack		- Hacker/Cracker - Competitor - Espionage	High	High	High
	Lack of operating system security	Stolen Data	- Competitor - Espionage	High	High	High
	Denial of Service, due to malware or directed attack	Loss of Availability	- Competitor - “Script Kiddies”	Low	Low	Low
	Data Modified, due to malware or directed attack	Loss of Data Integrity	- Competitor	High	High	High
			- “Script Kiddies”	Low	Low	Low
Lack of physical security	Stolen Laptop	- Loss of Data	-Competitor -Espionage	High	High	High
		- Loss of Availability	“Common” Criminals	Medium	Medium	Medium
	Lost Laptop		Owner/Employee	Low	High	Low
Regular wear & tear on equipment	Hard drive failure	- Loss of Data	n/a	Low	Low to High, depending on availability of backups	Low
	Damage to laptop (excluding hard drive)	- Loss of Data Integrity	Owner/Employee	Low		

Vulnerability	Threat	Damage	Source	Likelihood	Impact	Risk
Lack of regular backups	Permanent data loss in the event of hard drive failure	- Loss of Data	-Owner/Employee -IT Department	Low	High	Low
	Permanent data loss in the event of attack (directed), or stolen equipment		-Competitor -Espionage	High	High	High
	Permanent data loss in the event of un-directed attack (malware, virus, etc.)		“Script Kiddies”	Medium	Low	Low
	Partial data loss in the event of an accident or isolated “security event” (malware, virus, etc.)		-Owner/Employee -IT Department	Medium	Medium	Medium

Table 2 - Major asset that is directly affected

Affected Organizational Asset	Comments
Research and Development	Because this system (and others like it) will be used as researchers’ mobile workstations, R&D will be directly affected should the systems suffer any loss of Confidentiality, Integrity, or Availability.
Budget and Finance	Those familiar with research facilities/environment should be familiar with this concept. Budget at any research organization is inevitably linked to the ability of researchers to bring in funding, whether the source be the government or private companies.

1.3 – The References

What about the current state of practice? OS X has been on the market since 2001 (earlier, if you count the beta releases), so readers and users alike will be happy to know that there is plenty of information out there to facilitate putting together a secure configuration, though it may not always be easy to find. Here are some good sources that will be used in for the remainder of this exercise:

- Apple’s “An Introduction to Mac OS X Security”⁴ : A very good place to start, especially for those readers not necessarily familiar with UNIX conventions. This article starts off by explaining some UNIX terms and concepts (permissions, networking, etc.) and then goes into ways of securing the operating system. Though not a lengthy piece, OS X ships [relatively, of course] secure out of the box.
- Apple Security Updates⁵ : The authoritative list of security updates released by Apple for OS X (all versions, not just v10.3). At the time of this writing the latest update is dated 2/23/2004. This list can be used to confirm the patch status of the audit subject.
- CIS Benchmark for OS X⁶ : Best known for their security benchmark and scoring tools, CIS currently offers support for Windows NT & 2000, Solaris, Linux, and HP-UX. The “CIS Benchmark for OS X” project is an attempt to port the Linux tool over to OS X. Though still in the early stages of development, it is far enough along that the reports it generates can be used as a foundation for an audit checklist.
- CVE⁷ : Common Vulnerabilities and Exposures, which links vulnerabilities to a standardized name (e.g. “CAN-2004-0169”) – especially useful when trying to correlate data across multiple platforms, it allows the user to perform a search on a single common criteria and get back multiple (and most importantly, meaningful) results. Though it is not authoritative (and does not claim to be), CVE is also useful as a way to quickly reference in our case, Mac OS X and the list of disclosed vulnerabilities.
- Lawrence Berkeley National Laboratory⁸ : Has an excellent checklist for OS X posted on their web site.
- United States Department of Justice (USDOJ) Computer Crime and Intellectual Property Section (CCIPS)⁹ : For those based in the United States, this web site is invaluable. One can look up definitions (for example, what exactly is a ‘protected computer’?¹⁰), cases, laws, policies, etc. Those who are not attorneys will likely find the laws difficult to read and understand, but do not despair – there is much valuable information here.

⁴ <http://developer.apple.com/internet/security/securityintro.html>

⁵ <http://docs.info.apple.com/article.html?artnum=61798>

⁶ <http://sourceforge.net/projects/nitrogen>

⁷ <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mac+os+x>

⁸ http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html

⁹ <http://www.cybercrime.gov/>

¹⁰ <http://www.usdoj.gov/criminal/cybercrime/unlawful.pdf>

- Various web sites dedicated to Macintoshes and OS X¹¹: Not necessarily entirely security related, but these sites together contain a wealth of information for novice and expert Mac users alike.
- SANS InfoSec Reading Room¹² : Last, but certainly not least! The SANS Reading Room has some excellent articles under “Mac/Apple Issues”. Currently there are six papers available, and though there certainly is some overlap between them, as a group they provide quite the comprehensive collection of OS X best practices.

2.1 – The Checklist

The checklist to be used for the audit is provided in this section. The objective is to provide recommendations and instructions (to users and administrators alike) on how best to achieve a baseline level of security that Laboratory management would find acceptable. The focus will be on hardening the operating system to prevent unauthorized access, whether the potential intruders be local (physical access) or remote (over the network).

OSX10.3-1 – Login Banner	
Risk: Low	Corporate policy dictates that all systems connected to the network, if possible, must display a banner before the user logs in. The banner is used to warn potential intruders (“... authorized users only ...”), as well as employees (“... you may be monitored ...”). At least in the United States, banners may well contribute to the successful prosecution of unauthorized intruders ¹³
Testing Procedure and Compliance Criteria (Objective)	<ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select Log Out <Current User>. Or, simply restart the computer. 2. Verify that the text of the warning banner is displayed before users log in.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

¹¹ <http://www.macosxhints.com/>, <http://cerebus.sandiego.edu/~jerry/UnixTips/>, <http://www.osxfaq.com>, <http://www.macdevcenter.com>, <http://maccentral.macworld.com/>,

¹² http://www.sans.org/rr/catindex.php?cat_id=34

¹³ <http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm>

Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html • http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm
(continued) OSX10.3-1 – Login Banner	

OSX10.3-2 – Disable Auto-Login	
Risk: HIGH	By default, OS X will log the user in automatically upon startup, without prompting for a password. A serious vulnerability in and of itself, this problem is made worse by the fact that the default user account (created during the OS installation) has administrative rights.
Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Accounts. 4. Select Login Options. 5. The checkbox marked “Automatically Log in as: <username>” should be un-checked.
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Restart the system. 2. Verify that the system requires a password before logging in.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html

OSX10.3-3 – Disable Listing of Usernames in Login Window	
Risk: Low	If Auto-Login is disabled, the default behavior is to display a login window with a list of available users. While the user(s) will now have to type in a password to log in, it is still undesirable to have the list of users revealed before authentication, as this gives a potential intruder more information than is necessary.

Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Accounts. 4. Select Login Options. 5. For Display Login Window as:, “Name and password” should be selected (as opposed to “List of users”).
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Restart the system. 2. Verify that the system requires BOTH a username and a password to be entered into the dialog box before logging in. The username should not be presented in the form of a list that a user can simply click on.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html
(continued) OSX10.3-3 – Disable Listing of Usernames in Login Window	

OSX10.3-4 – Password Protected Screensaver	
Risk: Medium	We need to prevent unauthorized personnel from accessing the system when unattended. Due to the fact that these systems are expected to hold sensitive data, a password should be required in order to resume a session after the start of the screensaver.
Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Security. 4. Verify that Require password to wake this computer from sleep or screen saver is checked.

	<p>To verify system behavior:</p> <p>Time is valuable, so it's probably not the best idea to sit idle at the computer waiting for the screensaver to engage. Under OS X, it's possible to configure 'hot corners', where one can move the mouse cursor to any of the four corners of the screen to instantly activate the screensaver. To configure a hot corner,</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Desktop & Screen Saver. 4. Click on the button marked Hot Corners ... 5. Each of the four drop-down boxes represent a corner. Pick any drop-down, and select Start Screen Saver. <p>Once the hot corner has been configured, simply move the cursor into the configured corner. The screensaver will engage. Next, press any key or move the mouse again. The system should prompt you for a password before returning to the desktop.</p>
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
(continued) OSX10.3-4 – Password Protected Screensaver	

OSX10.3-5 – Screensaver Activation Time	
Risk: Medium	<p>In order for a locking screensaver to be useful, it needs to engage in a relatively short period of time after being left unattended. The longer the period before activation, the greater the exposure to potential intruders. Activation time needs to be balanced with convenience and usability – while you can easily set the screensaver to engage after 3 minutes of inactivity, users would surely end up spending the bulk of their time unlocking their systems as opposed to actually working.</p>
Testing Procedure and Compliance	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and

Criteria (Subjective)	select System Preferences . 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Desktop & Screen Saver . 4. Select Screen Saver . 5. Start Screen Saver: should be set to a relatively short period of time.
	To verify system behavior: Unfortunately, the only way to verify that the screensaver actually works is to wait. To shorten the wait, the auditor can shorten the amount of time before a screensaver is set to activate. To do this: 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences . 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Desktop & Screen Saver . 4. Move the slider marked start screen saver: to the shortest interval (3 minutes). 5. Verify that the screensaver activation mechanism is working. If so, the configured screensaver should activate after the system sits idle at around the three minute mark.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	• http://developer.apple.com/internet/security/securityintro.html
(continued) OSX10.3-5 – Screensaver Activation Time	

OSX10.3-6 – Disable Root Account	
Risk: Low	By default, the root account is disabled in OS X. During the installation a single user account is created, it being the single administrative account on the system. Here we are simply confirming that the user has left the root account disabled. As OS X generally provides the user multiple ways to accomplish administrative tasks, there is no operational need for an active root account.
Testing Procedure and Compliance	1. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 2. Double-click to open the Terminal application.

Criteria (Objective)	<p>3. At the prompt, type “nidump passwd . grep ^root”</p> <p>4. Verify that the result from the above command reads : “root:*:0:0::0:0:System Administrator:/var/root:/bin/sh”</p> <p>Note the single asterisk in the 2nd column (marked in red above) – this indicates that the root account is indeed disabled. If you see multiple asterisks (“*****”) or what looks like a crypt() hash (“VpHgNXnGe2bY”) it means the account has been enabled.</p>
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
(continued) OSX10.3-6 – Disable Root Account	

OSX10.3-7 – Use a Non-Privileged Account	
Risk: Low	During the installation of OS X, a single administrative account is created. Whenever possible, a non-privileged account should be created and used for daily tasks instead. This reduces the amount of damage caused in the event of an user error.
Testing Procedure and Compliance Criteria (Subjective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Accounts. 4. Verify that there is only one account labeled “Admin”, and that there is at least one other account labeled “Standard”. The user should be using the “standard” account for every day tasks.
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 2. Double-click to open the Terminal application. 3. At the prompt, type sudo echo test and hit <enter>. 4. When prompted for a password, enter the current user’s password. 5. Verify that the system responds with the following error, indicating that the current user is not allowed to execute sudo:

	<user> is not in the sudoers file. This incident will be reported.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
(continued) OSX10.3-7 – Use a Non-Privileged Account	

OSX10.3-8 – Remove Un-Necessary Accounts	
Risk: Low	The more accounts that exist on a system, the more potential entry points you have into a system. One single user with a weak password is all it takes for an intruder to gain access into your system. As we are dealing with a personal system, there should be few (if any) accounts that belong to anybody else but the owner.
Testing Procedure and Compliance Criteria (Subjective)	<ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Accounts. 4. Verify that each account listed belong to authorized users, and have a need to exist.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html

OSX10.3-9 – Use of Strong Passwords	
Risk: HIGH	All the security in the world can be nullified by a single user with a weak password. But until the world moves on to alternate forms of authentication (one time pads, smart cards, biometrics, etc.) passwords will continue to be a concern. The good news however, is that weak

	passwords can be rectified very easily, and with minimal effort.
Testing Procedure and Compliance Criteria (Subjective)	<p>1. Verify with the users that their passwords conform to the organization's password policy. If no corporate policy exists, plenty can be found on the Internet.</p> <p>Note : With the release of OS X v10.3 ("Panther"), Apple has made it more difficult than before to obtain password hashes. Additionally, they have also abandoned the use of crypt() as the default hashing function. All of this means that at this time, there are no known password crackers that can be used against Apple's new authentication method ("Shadow Hash"¹⁴), and this is why for the time being auditors will have to rely on purely administrative methods to audit this particular item. Those of you auditing previous versions of OS X (<= 10.2) can download a OS X port of John The Ripper here, complete with native Mac GUI interface.</p>
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://www.sans.org/resources/policies/Password_Policy.pdf • http://www.microsoft.com/technet/community/columns/5min/5min-302.msp • http://www.securityfocus.com/infocus/1537 • http://developer.apple.com/documentation/ ... • http://www.macosxhints.com/article.php?story=20031107215426990 • http://cerebus.sandiego.edu/~jerry/blog/article.php...
(continued) OSX10.3-9 – Use of Strong Passwords	

OSX10.3-10 – Home Folder Encryption	
Risk: HIGH	<p>A new feature in OS X v10.3, FileVault gives the user a secure and transparent way to encrypt all files in the user's home folder (this is similar to one's user profile directory in Windows NT/2K/XP). Once turned on, the user's home directory is converted to an image encrypted using AES-128. Encryption/decryption is done on the fly, requiring no user interaction. The value of using FileVault is that even in the event that someone has managed to steal the laptop and extracted the hard drive, the data would still be inaccessible.</p>

¹⁴http://developer.apple.com/documentation/Networking/Conceptual/Open_Directory/Preface/chapter_1_section_1.html

Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Security. 4. Verify that the system reports that FileVault protection is on for this account.
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Login as a user OTHER than the account being audited. For example, if you're auditing user account 'jfung', log in instead as another account (e.g. 'adminjfung') 2. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 3. Double-click to open the Terminal application. 4. At the prompt, change to the target account: cd ~jfung. 5. List the contents of the user's home directory (ls -la), and verify that the only file listed is <username>.sparseimage (you will see multiple files and directories if the home directory is not encrypted).
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://www.macdevcenter.com/pub/a/mac/2003/12/19/filevault.html • http://www.apple.com/macosx/features/filevault/
(continued) OSX10.3-10 – Home Folder Encryption	

OSX10.3-11 – Install Anti-Virus Software	
Risk: Low	<p>As a general rule, OS X users need not worry about viruses/Trojans¹⁵ nearly as much as users of Microsoft Windows (because the vast majority of the malware out there in the wild still targets Windows systems and applications). Nevertheless, anti-virus solutions do exist for OS X and should be installed. On April 8th 2004 Intego¹⁶ announced that they had updated virus definitions for the first known Trojan horse for Mac OS X, dubbed "MP3Concept". Though only a proof-of-concept, MP3Concept nevertheless serves as a wake up call to those in Mac communities who long believed OS X to be somehow</p>

¹⁵ http://www.webopedia.com/TERM/T/Trojan_horse.html

¹⁶ <http://www.intego.com/home.asp>

	immune to viruses and other forms of malware.
Testing Procedure and Compliance Criteria (Objective)	<ol style="list-style-type: none"> 1. Download the Eicar¹⁷ test file. 2. Verify that the anti-virus software correctly detects this file.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html • http://www.intego.com/news/pr40.html
(continued) OSX10.3-11 – Install Anti-Virus Software	

OSX10.3-12 – Software Update Frequency	
Risk: Low	OS X has a built-in Software Update application similar to Microsoft's Windows Update. The application will check Apple's site and present the user with a choice of updates to install. By default, Software Update will automatically check for updated versions of the various components installed with OS X on a weekly basis. While not every update is necessarily security-related, making sure Software Update is enabled and set to update frequently is a simple and effortless way for the user to keep informed about the latest patches.
Testing Procedure and Compliance Criteria (Objective)	<ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Software Update. 4. Verify that the Check for updates: is enabled (checkbox checked), and the interval is set to Daily.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html

¹⁷ http://www.eicar.org/anti_virus_test_file.htm - For those unfamiliar, this is a 'test virus' distributed by the European Institute for Computer Anti-Virus Research, and is a safe way of testing your AV product.

OSX10.3-13 – Patch, Patch, Patch!	
Risk: HIGH	Apple issues updates on a fairly regular basis to address various software bugs and vulnerabilities that are an accepted part of today's complex operating systems. Un-patched systems are a threat not only to themselves, but also to the other systems on the network. This is especially important for laptops, because they will travel from network to network (work ⇔ home, for instance) on a regular basis, and will be subject to harsher network environments than your average corporate server or desktop.
Testing Procedure and Compliance Criteria (Objective)	<ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select Software Update, and click the Check Now button. 2. Verify that all updates have been installed.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html

OSX10.3-14 – Central System Logs (syslog)	
Risk: Low	In the event of a compromise, system logs will play a vital role in the re-construction of the crime scene. The problem here is that once a system has been compromised, none of the data on the system can be trusted, including the system logs. While there are multiple ways to mitigate this problem ¹⁸ , one of the 'cheapest' ways to do so is to automatically forward a workstation's logs to a central system log server. This way, should an intruder manage to break into a system and alter its logs, a pristine copy will already have been stored on the central server and could still be used for network forensics.
Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 2. Double-click to open the Terminal application. 3. At the prompt, type cat /etc/syslog.conf. Verify that the logs are

¹⁸ <http://www.schneier.com/paper-auditlogs.html>

	<p>being forwarded to the designated central log host (indicated by an “@” in front of the name, e.g. “@loghost.localdomain”).</p>
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 2. Double-click to open the Terminal application. 3. At the prompt, type /usr/bin/logger This is a test. 4. Verify that the message “This is a test” appears on the remote log server. <p>- An alternate to step 4 above would be to use a network packet sniffer (tcpdump, ethereal, etc.) to monitor the wire as you generate the log message. This method may be useful in cases where the auditor does not have easy access to the central log server, but still needs to verify that the workstation is configured for remote logging. This method is demonstrated in Part 3.</p>
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://www.cert.org/tech_tips/intruder_detection_checklist.html • http://project.honeynet.org/papers/enemy2/ • http://www.schneier.com/paper-auditlogs.html • http://www.cs.colorado.edu/%7Etor/sadocs/misc/syslog.html
(continued) OSX10.3-14 – Central System Logs (syslog)	

OSX10.3-15 – TCP Wrappers	
Risk: Medium	<p>Also bundled with OS X, Wietse Venema’s venerable TCP Wrappers package is long familiar to UNIX/Linux users. In its most basic form, TCP Wrappers will provide additional information in your system logs as to who’s connecting and where from. Properly configured, you will have the ability to control access at the host, domain, subnet, or service level. It should be noted that TCP Wrappers should be used <i>in addition to</i>, not in place of, a firewall (think “Defense In-Depth”). In addition, the default behavior should be set to “default deny”, similar to firewalls.</p>

Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click hard drive icon on the desktop (default: Macintosh HD) → Applications → Utilities 2. Double-click to open the Terminal application. 3. At the prompt, type cat /etc/hosts.deny 4. Verify that the only uncommented line reads ALL:ALL
	<p>To verify system behavior:</p> <p>To test for the existence of TCP Wrappers, we'll need to try and connect to a service on our test system from another system on the network. FTP & SSH are generally good candidates for this kind of test. If neither services is currently activated on the system, we can temporarily activate it for the duration of this test (which should take less than a couple of minutes). A crossover cable may be used to ensure that no system other than the intended client may connect to this service during this window. To activate SSH:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Sharing. 4. Turn on Remote Login. <p>Now on the remote computer:</p> <ol style="list-style-type: none"> 1. Telnet to the test system, port 22 (e.g. telnet 1.2.3.4 22) 2. Verify that the system connects, then immediately closes connection <i>without</i> ever displaying the SSH banner (which reveals the SSH version, e.g. "SSH-2.0-OpenSSH_3.8p1").
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://www.osxfaq.com/man/8/tcpdmatch.ws • ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB • http://www.apple.com/opensource/
(continued) OSX10.3-15 – TCP Wrappers	

OSX10.3-16 – Disable Un-Necessary Network Services	
Risk: Medium	As OS X is based on FreeBSD ¹⁹ , users now have the ability to run a plethora of open-source applications unavailable to those users of “Classic Mac OS” (< v10.0). In fact, OS X comes bundled with Apache, Samba, OpenSSH, plus an FTP daemon, just to name a few. While convenient, this also means that OS X users are subject to the same vulnerabilities that plague the rest of the open-source community. ²⁰ While these services are not enabled by default, it is extremely easy for a user to enable them without knowing significance of having enabled Apache, for instance.
Testing Procedure and Compliance Criteria (Subjective)	To verify system setting; <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Sharing. 4. Click on Services, if not already selected. 5. Verify that only those services required are actually active.
	To verify system behavior: <ol style="list-style-type: none"> 1. Use a network port scanner (nmap²¹ comes to mind) to scan the system in question. 2. Verify that only the ports running necessary services report back as ‘open’.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
(continued) OSX10.3-16 – Disable Un-Necessary Network Services	

OSX10.3-17 – Enable the Firewall	
Risk: Medium	OS X does come with a built-in firewall, ipfw, though disabled by default. As secure as OS X is purported to be, a firewall is <i>always</i> a good idea.

¹⁹ <http://developer.apple.com/unix/>

²⁰ <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=macos>

²¹ <http://www.insecure.org/>

Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Sharing. 4. Select Firewall. 5. Verify that the firewall is active (“Firewall On”).
	<p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. Use a network port scanner to scan all the ports on the system in question (nmap recommended). 2. Verify that only the ports running necessary services report back as ‘open’. 3. Verify that all the other ports return a status of ‘filtered’, as opposed to ‘closed’. Note that ‘filtered’ vs. ‘closed’ is nmap nomenclature, if you use a different scanner the returned status may be labeled differently. Nmap labels a port as ‘filtered’ when it receives zero response for its attempt to connect. If instead it receives a TCP RST when trying to make a connection, that port is considered ‘closed’.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://developer.apple.com/internet/security/securityintro.html • http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
(continued) OSX10.3-17 – Enable the Firewall	

OSX10.3-18 – Bluetooth Discovery and Authentication	
Risk: Low	<p>Apple PowerBooks come equipped with both 802.11g (Airport Extreme) as well as Bluetooth support. By default, the Bluetooth adapter is configured to allow itself to be discovered by other devices. Bluetooth vulnerabilities, while relatively few at this point, are becoming more serious and prevalent²². If Bluetooth support is needed, users should disallow the remote discovery of their Bluetooth device (in this case, the PowerBook), as well as require authentication and</p>

²² <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0143>

	encryption for those devices connected.
Testing Procedure and Compliance Criteria (Objective)	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences. 2. Click on Show All at top left-hand corner of the System Preferences window, to display all available options. 3. Select Bluetooth 4. Verify that Discoverable is un-checked, and Require Authentication and Use Encryption are both checked. <p>To verify system behavior:</p> <ol style="list-style-type: none"> 1. To check if Bluetooth Discovery has been disabled on the PowerBook, you will need a 2nd Bluetooth device capable of performing discoveries (e.g. a PDA, laptop, etc.). 2. On the 2nd Bluetooth device, perform a discovery (actual method will differ based on device/software/vendor), and verify that the PowerBook does not appear on any list of discovered devices.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> • http://maccentral.macworld.com/news/2004/02/11/bluetooth/ • http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0143
(continued) OSX10.3-18 – Bluetooth Discovery and Authentication	

OSX10.3-19 – WiFi Automatic Discovery and Association	
Risk: Medium	Apple PowerBooks come equipped with both 802.11g (Airport Extreme) as well as Bluetooth support. By default, the WiFi adapter is set to automatically join any available network. This should be discouraged as any network that can be attached to automatically will not have any encryption (WEP) enabled, and eavesdroppers will be able to intercept data sent across the airwaves. Additionally, as the default behavior is to obtain information from a DHCP server, malicious individuals will be able to set up an AP configured with their settings and route all those who associate with their AP through their systems of choice, a perfect set up for a DNS spoof/session hijack/Man-in-the-middle/exploit-of-the-week attack.
Testing Procedure and Compliance Criteria	<p>To verify system setting:</p> <ol style="list-style-type: none"> 1. Click the Apple icon on the top left-hand corner of the desktop, and select System Preferences.

(Objective)	<ol style="list-style-type: none"> Click on Show All at top left-hand corner of the System Preferences window, to display all available options. Select Network. For each Location (default is Automatic), verify that AirPort is set to By default, join: A specific network.
	<p>To verify system behavior:</p> <p>To confirm that your test system will not simply associate to the first available access point, you will need to set up a dummy AP. This can be done with a real AP (cheap ones can be purchased for well under \$100), or those Linux-savvy can use their laptops equipped with an Intersil Prism WiFi card to simulate an AP²³.</p> <ol style="list-style-type: none"> Whichever way you choose to stand up an access point, the key here is to turn <i>off</i> all the security features. E.g. No WEP, no MAC address filtering, turn <i>on</i> SSID broadcast, etc. Verify that the PowerBook does NOT attempt to connect to the dummy AP.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1009 http://www.cs.ndsu.nodak.edu/~karg/Malicious%20Attacks%20of%20Wireless%20Access%20Points.ppt http://www.securiteam.com/securitynews/6K0050A95S.html
(continued) OSX10.3-19 – WiFi Automatic Discovery and Association	

OSX10.3-20 – Backups	
Risk: HIGH	Unfortunately, OS X does not include a real backup utility. A quick search through the built-in help documents revealed that the current suggestion for backing up data is the burn it onto optical media (DVD or CD). Whatever the method, users should a reliable way of backing up and restoring their critical data.
Testing Procedure and Compliance Criteria (Subjective)	<ol style="list-style-type: none"> Verify with the user that they have a regular backup scheme in place. Attempt to restore a file from the last backup and verify file integrity if possible (do md5sums exist? Etc.).

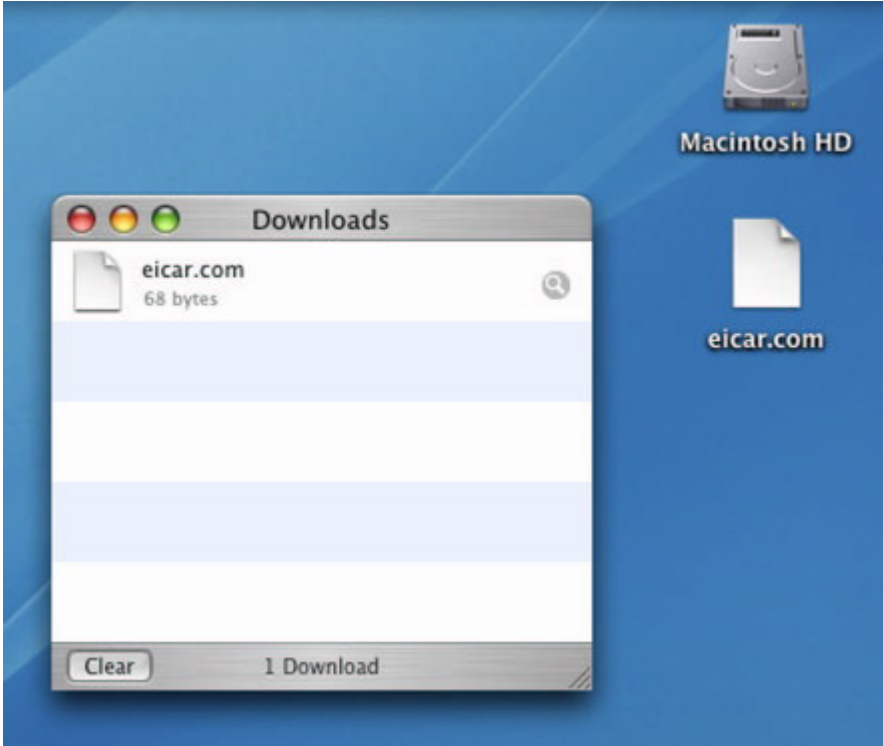
²³ <http://hostap.epitest.fi/>

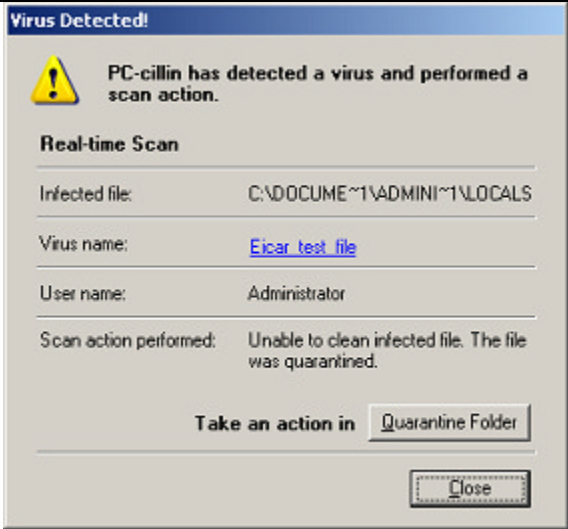
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> Mac OS Help (built-in to OS X)
(continued) OSX10.3-20 – Backups	

OSX10.3-21 – Open Firmware Password	
Risk: Medium	<p>Once an intruder obtains physical access to a system, it is only a matter of time before they gain access to the data on that system. With a Firmware password set, we're trying to increase the amount of time it will take an intruder to get into the system, with the hope that it will stall them long enough that they can be detected (and stopped), or that it makes the task of breaking into our system difficult enough as to not be worth their efforts (think time-based security). Those familiar with x86 PC hardware will recognize this as very similar to the "BIOS boot password" available on just about every PC out there. The principle is similar, but on a Mac this will disable all startup hotkey sequences, thereby preventing unauthorized users from booting from a device other than your specified boot media without a password, as well as preventing the startup into single-user mode via the special key sequences.</p>
Testing Procedure and Compliance Criteria (Objective)	<ol style="list-style-type: none"> 1. Restart the system and hold down the Command and S keys, to attempt to boot into single-user mode. Verify that the system starts up as normal (never going into single-user mode). 2. Restart the system with a bootable CD in the CD-ROM drive, and hold down the C key. Mac users will recognize this as the key sequence needed to boot the system from the CD. Verify that the system boots up as normal (without going to the CD). 3. Restart the system with a bootable CD in the CD-ROM drive, and hold down the Option key. Verify that a password is required before allowing you to select an alternate boot device.
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank
Reference(s)	<ul style="list-style-type: none"> http://www.apple.com/support/downloads/openfirmwarepassword.html http://docs.info.apple.com/article.html?artnum=120095

3.1 – The Audit

With the checklist finished, we now move on to the actual testing. For this section, we'll choose 10 items out of the checklist developed in Part 2. Because the full description has already been listed above, we will only be listing the Evidence and Findings sections here.

Test Item #1 : OSX10.3-11 – Install Anti-Virus Software	
Evidence:	<p>To test for the existence of anti-virus software, we attempt to download the Eicar test file from www.eicar.org.</p>  <p>The screenshot shows a Mac OS X desktop with a blue background. In the center, there is a 'Downloads' window from Safari. The window title is 'Downloads' and it shows a single file named 'eicar.com' with a size of '68 bytes'. Below the file list, there is a 'Clear' button and a status bar that says '1 Download'. On the desktop, to the right of the window, there is a file icon labeled 'eicar.com'.</p> <p>Figure 1 - Download of eicar.com using Safari (Apple's web browser)</p>
Finding: FAIL	<p>Notice that the file successfully downloaded onto the desktop. The desired behavior would have been for the anti-virus software to intercept the file before it was written to the desktop, as illustrated here with an anti-virus package running under Windows XP:</p>

	 <p>This did not happen on our test system, indicating that anti-virus software does NOT exist.</p>
(continued) Test Item #1 : OSX10.3-11 – Install Anti-Virus Software	

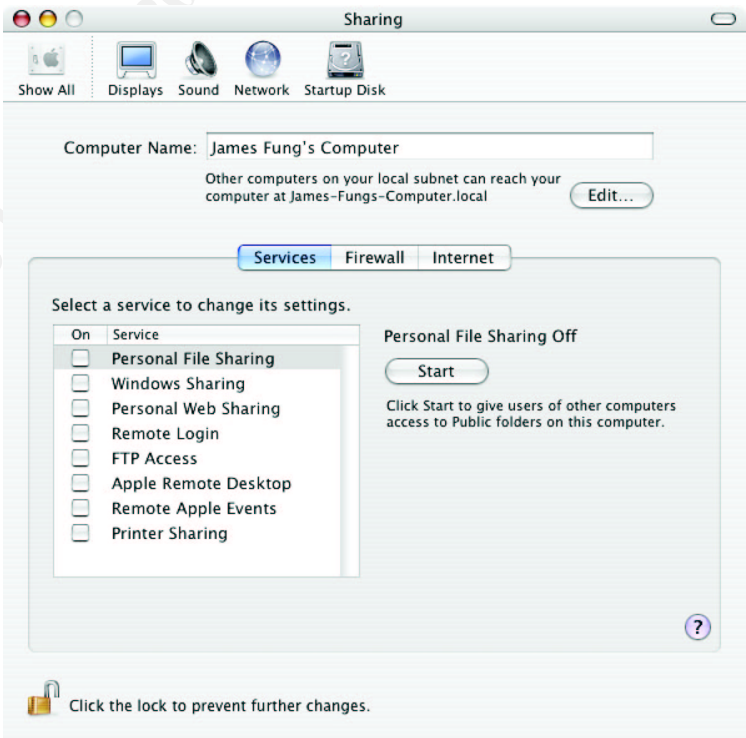
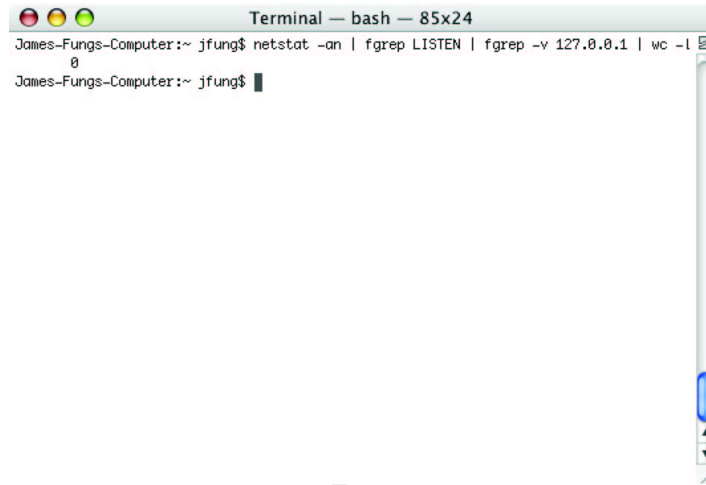
Test Item #2 : OSX10.3-16 – Disable Un-Necessary Network Services	
Evidence:	<ol style="list-style-type: none"> First, we check system preferences to see if any of the built-in services have been started: 

Figure 2 - System Preferences à Sharing

2. Next, we use the **netstat**²⁴ locally to determine if there might be any network services listening that are not controlled via the system preferences GUI interface.

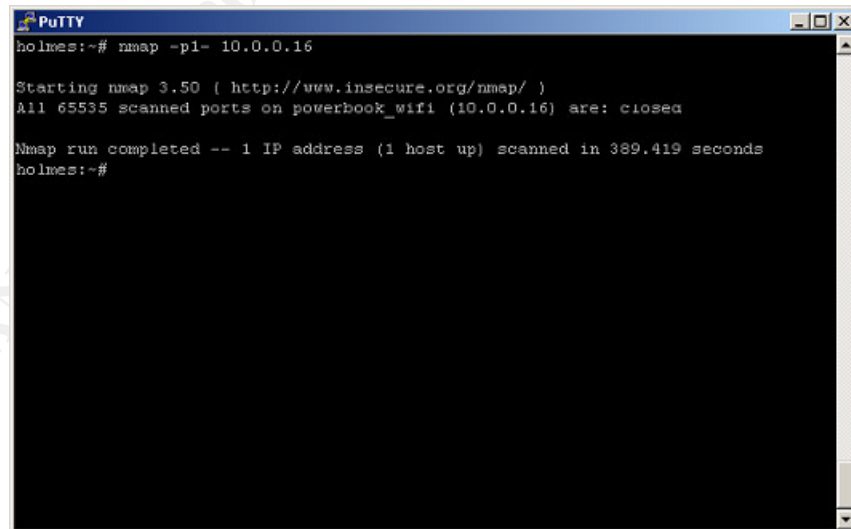


```
Terminal — bash — 85x24
James-Fungs-Computer:~ jfung$ netstat -an | fgrep LISTEN | fgrep -v 127.0.0.1 | wc -l
8
James-Fungs-Computer:~ jfung$
```

Figure 3 - Netstat

Evidence
(Cont.)

3. Finally, we use **nmap**²⁵ to conduct a port scan of the system, as confirmation.



```
PuTTY
holmes:~# nmap -p1- 10.0.0.16

Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
All 65535 scanned ports on powerbook_wifi (10.0.0.16) are: closed

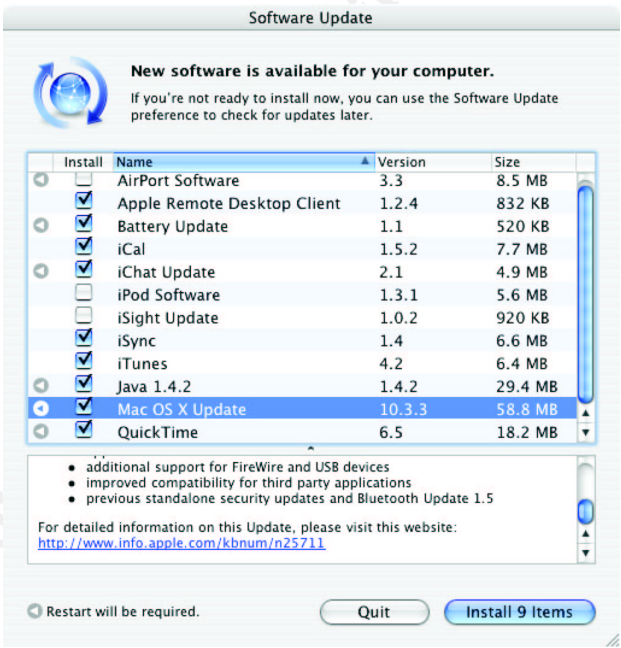
Nmap run completed -- 1 IP address (1 host up) scanned in 389.419 seconds
holmes:~#
```

Figure 4 – Nmap

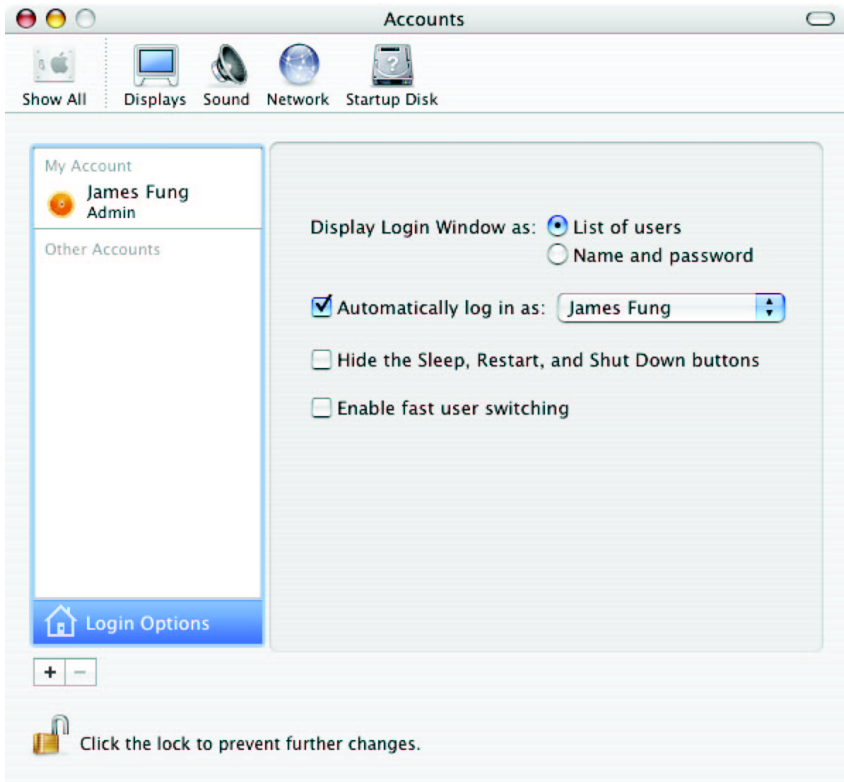
²⁴ <http://developer.apple.com/documentation/Darwin/Reference/ManPages/html/netstat.1.html>

²⁵ <http://www.insecure.org/nmap/>

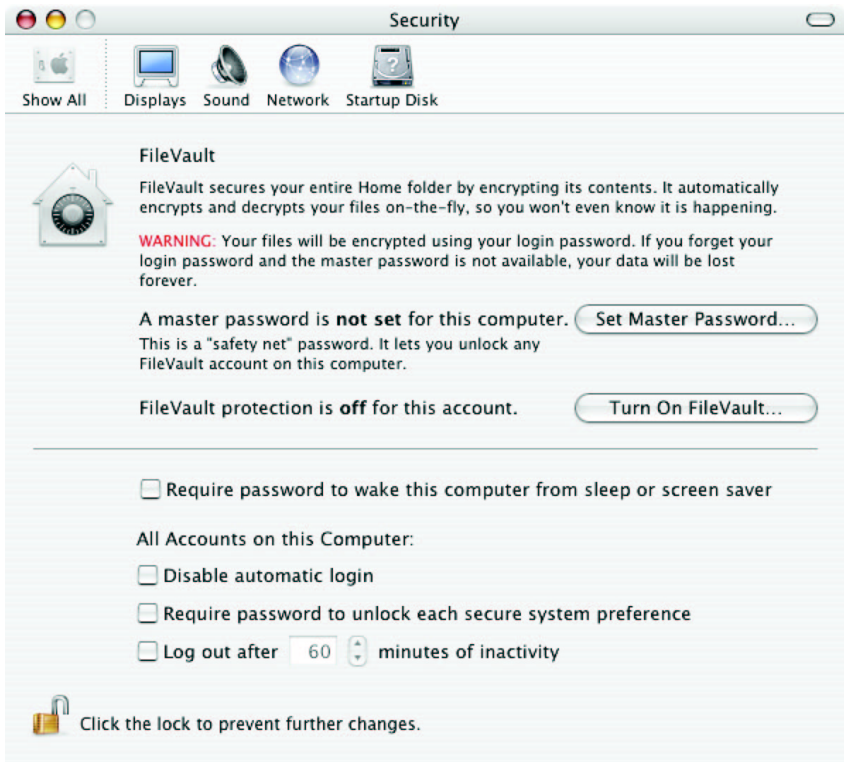
<p>Finding: Pass</p>	<p>This system passes all three tests:</p> <ol style="list-style-type: none"> 1. None of the built-in services have been enabled, as shown in Figure 2. 2. The netstat command confirms the above findings, and also tells us that there are no services listening on any of the network interfaces. This is important because a user can enable services without using the provided GUI. 3. Finally, a port scan initiated from another system on the network serves to confirm what was reported by netstat locally, a sanity check.
<p>(continued) Test Item #2 : OSX10.3-16 – Disable Un-Necessary Network Services</p>	

<p>Test Item #3 : OSX10.3-13 – Patch, Patch, Patch!</p>	
<p>Evidence:</p>	<p>To verify that all available patches have been installed, we go to System Preferences → Software Update → Check Now:</p>  <p>Figure 5 - OS X Software Update</p>
<p>Finding: FAIL</p>	<p>Figure 5 shows that there are at least 9 separate updates that have yet to be installed. While not all of those updates listed are security-related, it is nevertheless recommended that system updates be installed as soon as they are made available by Apple.</p>

Test Item #4 : OSX10.3-2 – Disable Auto-Login

Evidence:	<p>To verify that auto-login has been disabled, we go to System Preferences → Accounts → Login Options:</p>  <p>Figure 6 - Login Options</p>
Finding: FAIL	<p>As seen in Figure 6, auto-login is indeed enabled for this system. This comes as no surprise as this is the default system behavior. Users are <i>strongly</i> encouraged to disable this setting immediately!</p>

Test Item #5 : OSX10.3-10 – Home Folder Encryption

Evidence:	<p>1. To verify that encryption (FileVault) has been enabled, we first go to System Preferences → Security:</p>  <p>Figure 7 – Security preferences</p> <p>2. Next, we reboot into single user mode by holding down command-s during the boot sequence. We then change to the user's home directory and attempt to list some files:</p> <pre>localhost:/ root# cd /Users/jfung localhost:/Users/jfung root# ls -la grep ^d total 40 drwxr-xr-x 15 501 501 510 28 Mar 17:45 . drwxrwxr-t 5 root admin 170 15 Mar 18:32 .. drwx----- 7 501 501 238 28 Mar 19:31 .Trash drwx----- 6 501 501 204 28 Mar 19:31 Desktop drwx----- 3 501 501 102 15 Mar 18:32 Documents drwx----- 23 501 501 782 28 Mar 17:00 Library drwx----- 3 501 501 102 15 Mar 18:32 Movies drwx----- 3 501 501 102 15 Mar 18:32 Music drwx----- 3 501 501 102 15 Mar 18:32 Pictures drwxr-xr-x 4 501 501 136 15 Mar 18:32 Public drwxr-xr-x 5 501 501 170 15 Mar 18:32 Sites localhost:/Users/jfung root#</pre>
Finding: FAIL	<p>1. As seen in Figure 7, FileVault is <i>not</i> enabled.</p> <p>2. To confirm that this is indeed the case, we booted into single user mode and confirmed that the root account was able to read the contents of the</p>

	<p>user's home directory. Had FileVault been enabled, all that would be seen by root would have been a single encrypted image file (a 'sparse image'), as seen here:</p> <pre>localhost:/ root# cd /Users/jfung localhost:/Users/jfung root# ls -la ^grep ^d drwxr-xr-x 3 501 501 102 28 Mar 19:46 . drwxrwxr-t 5 root admin 170 28 Mar 19:48 .. localhost:/Users/jfung root# ls -la total 98560 drwxr-xr-x 3 501 501 102 28 Mar 19:46 . drwxrwxr-t 5 root admin 170 28 Mar 19:48 .. -rwxr--r-- 1 501 501 50458624 28 Mar 19:48 jfung.sparseimage localhost:/Users/jfung root# file jfung.sparseimage jfung.sparseimage: data localhost:/Users/jfung root#</pre>
(continued) Test Item #5 : OSX10.3-10 – Home Folder Encryption	

Test Item #6 : OSX10.3-9 – Use of Strong Passwords	
Evidence:	<p>As there is currently no password cracker that can handle Panther's password hashes, the auditor will have to either trust the users who say their passwords comply, or develop their own password cracker. Here is a simple perl script that accepts a single command-line argument (the wordlist, one word per line) and attempts a dictionary attack on the current user's password: (comments in brown)</p>

© SANS Institute 2004

Here is the actual execution of the script:



(continued) **Test Item #6 : OSX10.3-9 – Use of Strong Passwords**

35

Test Item #7 : OSX10.3-17 – Enable the Firewall

1. To verify that OS X's built-in firewall has been enabled, we first go to System Preferences → Sharing → Firewall:

Evidence:

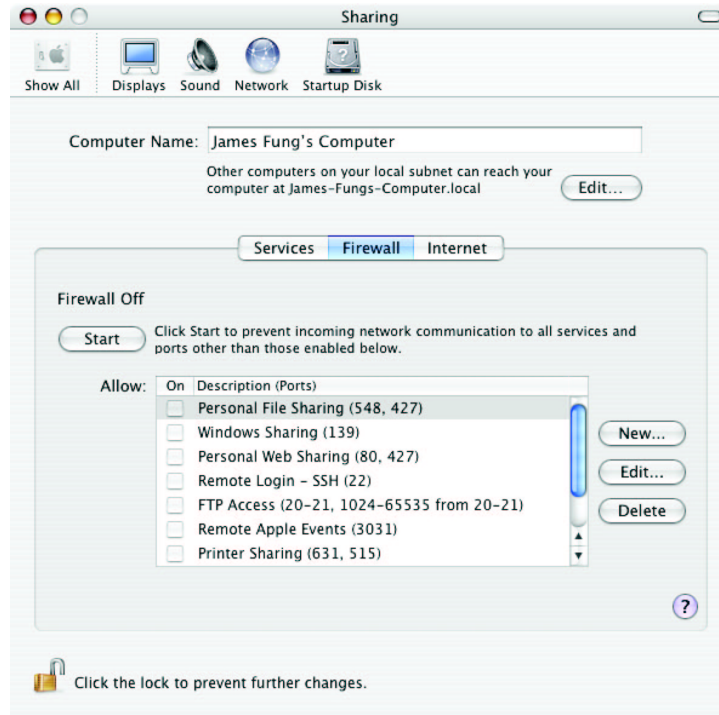


Figure 8 - Notice that the firewall is off

2. Next, we conduct an nmap scan of the PowerBook.

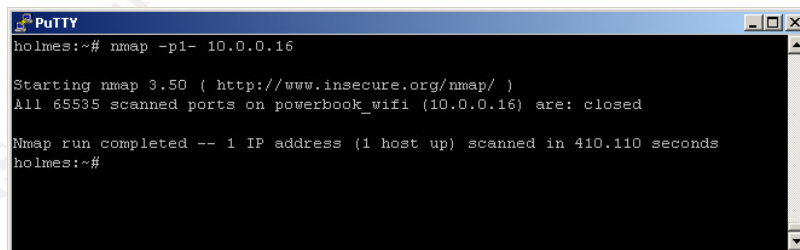
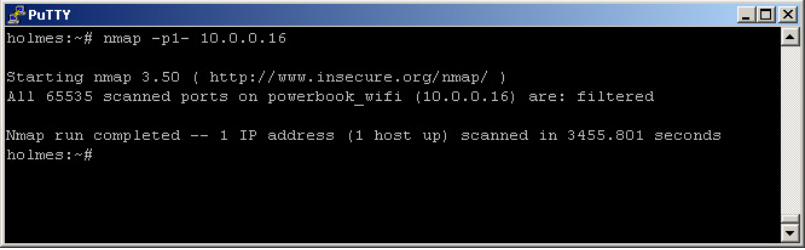
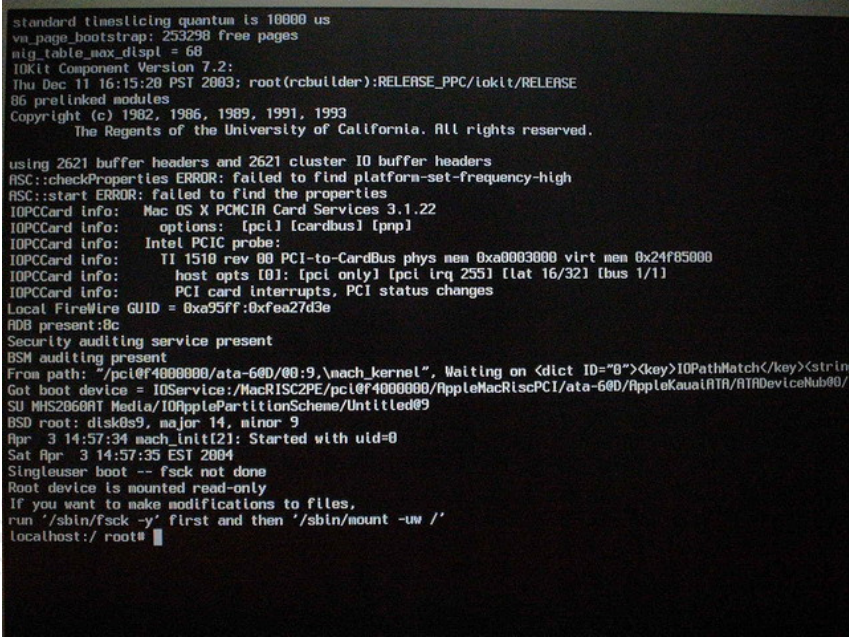


Figure 9 - All ports are closed

Finding:
FAIL

As seen in Figure 8 and confirmed in Figure 9, the firewall was indeed disabled. On a firewalled system, we would expect to see the ports come back as 'filtered', not 'closed'. In addition, the actual scan itself will take much longer as nmap no longer receives any confirmation as to whether a port is open or not. Below is a screenshot of what a firewalled system would look like to nmap:

	 <p>holmes:~# nmap -p1- 10.0.0.16</p> <p>Starting nmap 3.50 (http://www.insecure.org/nmap/) All 65535 scanned ports on powerbook_wifi (10.0.0.16) are: filtered</p> <p>Nmap run completed -- 1 IP address (1 host up) scanned in 3455.801 seconds holmes:~#</p> <p>Figure 10 - Firewall Enabled: scan takes much longer, and everything's filtered</p>
(continued) Test Item #7 : OSX10.3-17 – Enable the Firewall	

Test Item #8 : OSX10.3-21 – Open Firmware Password	
Evidence:	<ol style="list-style-type: none"> To verify that a password has been assigned, we restarted the PowerBook and held down the command and S keys, to attempt to boot into single-user mode. The result was as follows: <div data-bbox="483 909 1328 1543">  </div> <p>Figure 11 - Notice we are sitting at a root prompt, without ever authenticating!</p> Next, we attempt to boot the system with OS X Installation CD #1 by inserting the CD and restarting the system, this time holding down the C key.

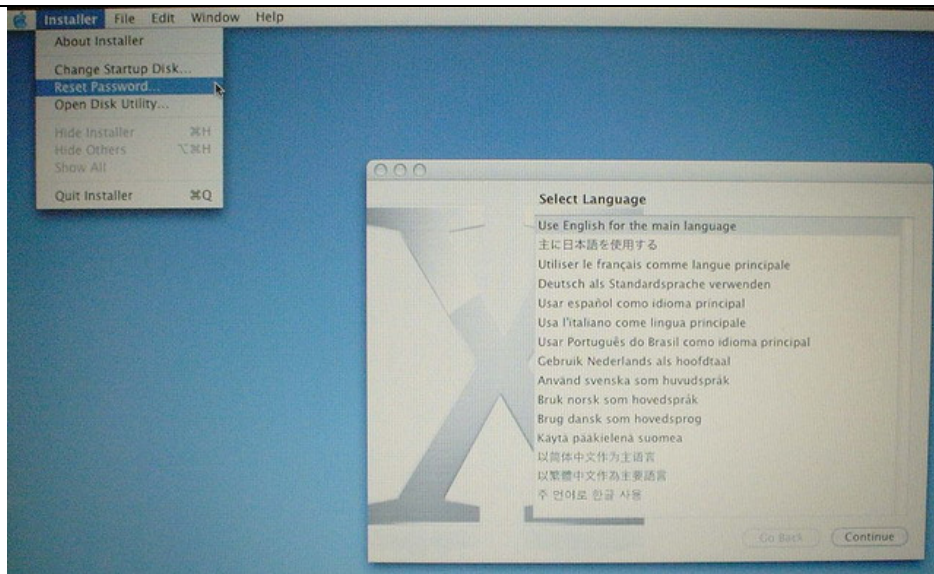


Figure 12 - Notice the "Reset Password" option ...

3. Finally, with Install CD #1 still in the system, we rebooted the system and held down the **option** key. We were greeted with the following boot menu:

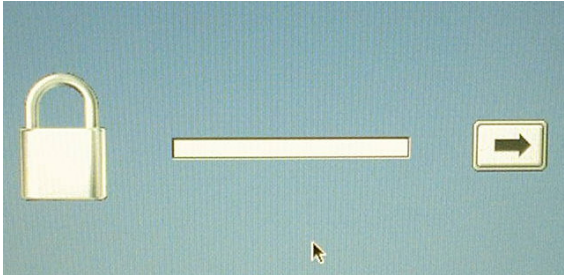


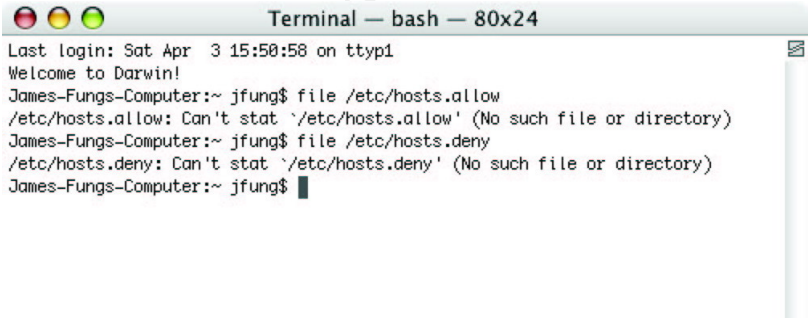

Figure 13 - Boot Menu

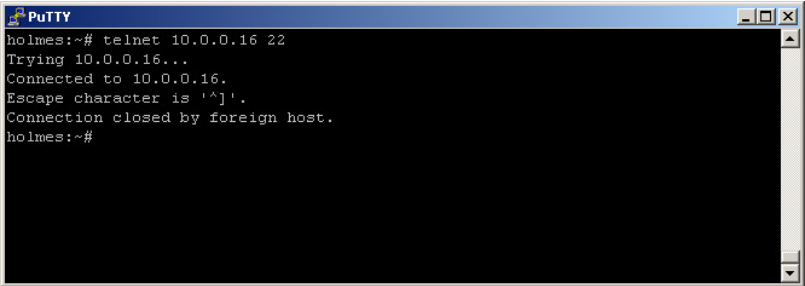
We selected "Mac OS X Install Disc 1" and then clicked the right arrow on the screen, and confirmed that we were able to boot off the CD without a password.

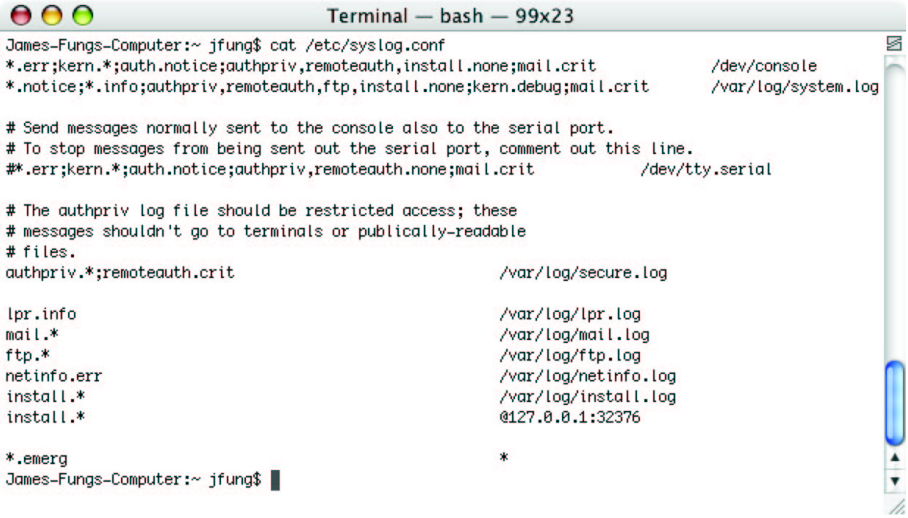
Finding:
FAIL

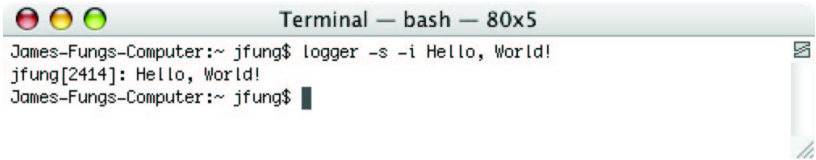
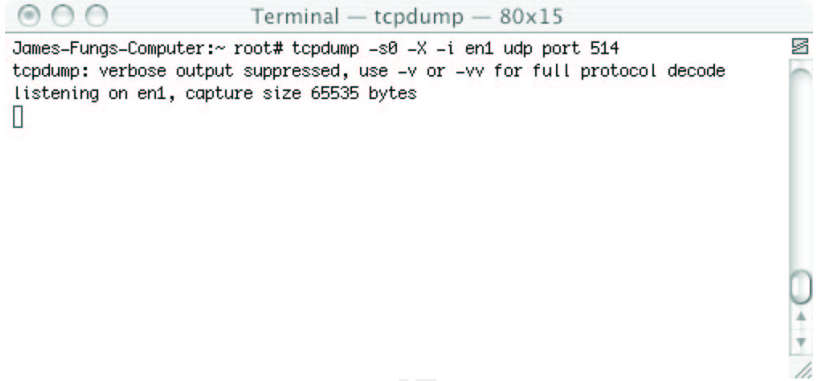
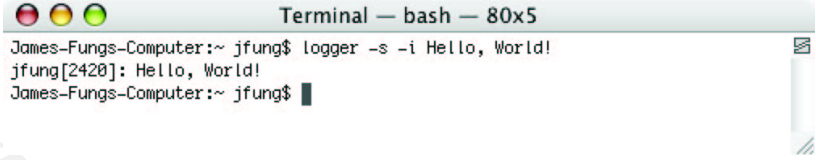
As seen in Figure 11, we successfully started into single-user mode simply by holding down the correct key combination at start up – no authentication required! This is especially of concern on laptops, where mobility means an increased chance of being stolen. Tests two and three help to confirm that no Open Firmware password exists on this system. Had a password been set, tests one and two would have failed (both boot attempts would have gone straight to the OS installed on the hard drive), and test three would have resulted in a password prompt before the boot menu was presented to the user, as seen in Figure 14:

	 <p data-bbox="690 514 1120 546">Figure 14 - Open Firmware Password</p>
(continued) Test Item #8 : OSX10.3-21 – Open Firmware Password	

Test Item #9 : OSX10.3-15 – TCP Wrappers	
Evidence:	<ol style="list-style-type: none"> <li data-bbox="462 787 1388 892">1. The easiest way to check for the use of TCP Wrappers is to look for the access control tables, /etc/hosts.allow and/or /etc/hosts.deny. As we see below, neither file exists: <div data-bbox="503 934 1307 1249">  <pre data-bbox="503 966 1234 1123"> Last login: Sat Apr 3 15:50:58 on ttty1 Welcome to Darwin! James-Fungs-Computer:~ jfung\$ file /etc/hosts.allow /etc/hosts.allow: Can't stat '/etc/hosts.allow' (No such file or directory) James-Fungs-Computer:~ jfung\$ file /etc/hosts.deny /etc/hosts.deny: Can't stat '/etc/hosts.deny' (No such file or directory) James-Fungs-Computer:~ jfung\$ </pre> <p data-bbox="722 1270 1079 1302">Figure 15 - No TCP Wrappers?</p> </div> <ol style="list-style-type: none"> <li data-bbox="462 1354 1388 1459">2. To confirm that TCP Wrappers are not being used, ssh was enabled on the PowerBook and an attempt is made to connect to port 22. The results are as follows: <div data-bbox="503 1491 1307 1774">  <pre data-bbox="503 1522 876 1701"> holmes:~# telnet 10.0.0.16 22 Trying 10.0.0.16... Connected to 10.0.0.16. Escape character is '^]'. SSH-1.99-OpenSSH_3.6.1p1+CAN-2003-0693 ^] telnet> quit Connection closed. holmes:~# </pre> <p data-bbox="470 1795 1339 1827">Figure 16 - Notice, that we are able to connect and see the OpenSSH banner</p> </div>

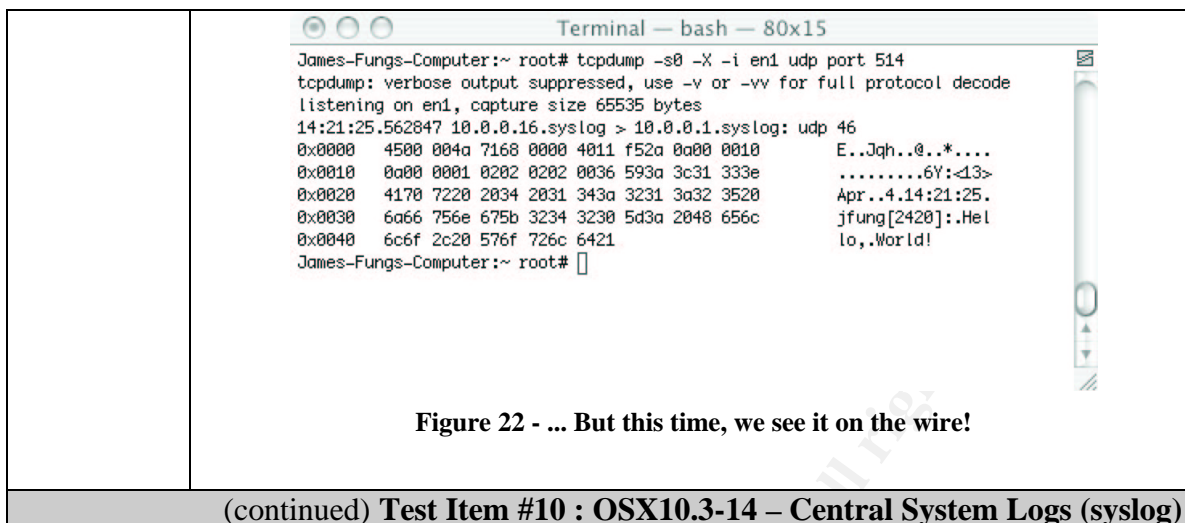
<p>Finding: FAIL</p>	<p>It was confirmed that TCP Wrappers were not configured on this system. First, we confirmed that neither /etc/hosts.allow or /etc/hosts.deny exist on the system. Next, in test #2 we were able to connect to port 22 (used by ssh) and retrieve the banner information ('SSH-1.99-OpenSSH_3.6.1p1+CAN-2003-0693'). If a system is properly 'wrapped', the connection would be closed immediately after connection, as follows:</p>  <p>Figure 17 - With TCP Wrappers properly configured, the connection is dropped immediately (notice the lack of banner information).</p>
(continued) Test Item #9 : OSX10.3-15 – TCP Wrappers	

Test Item #10 : OSX10.3-14 – Central System Logs (syslog)	
<p>Evidence:</p>	<ol style="list-style-type: none"> To check to see if the system is currently configured to send its logs to a remote log server, we first take a peek at /etc/syslog.conf:  <p>Figure 18 - Notice the only entry beginning with an '@' sign is localhost ...</p> <ol style="list-style-type: none"> To confirm, we will generate our own syslog messages, at the same time capturing the network traffic with a packet sniffer. The results are as follows:

	 <p>Figure 19 - We generate our syslog message ...</p>  <p>Figure 20 - ... And at the same time monitor the network for signs of logs leaving the system</p>
<p>Finding: FAIL</p>	<p>While /etc/syslog.conf did contain one entry where the destination started with an '@' sign, the destination host was in fact the localhost (127.0.0.1), indicating that no logs were being sent to a remote host. This was confirmed in test two, where we generated our own syslog message with logger²⁷ and captured all syslog packets coming to/from the system at the same time with tcpdump²⁸. Had remote logging been enabled, tcpdump would have captured the log packets leaving our system:</p>  <p>Figure 21 - We once again generate our syslog message ...</p>

²⁷ <http://developer.apple.com/documentation/Darwin/Reference/ManPages/html/logger.1.html>

²⁸ <http://developer.apple.com/documentation/Darwin/Reference/ManPages/html/tcpdump.1.html>



4.1 – The Summary

The focus of this audit was an Apple PowerBook laptop running what amounted to a default installation of the latest version of Mac OS X (dubbed ‘Panther’). This system is an exact duplicate of those currently being issued to the research scientists, thus their security is of special concern to the organization. The objective of this audit was to determine what threats our scientists were being exposed to by using these laptops, and how best to eliminate (or at the very least, mitigate) the risks involved.

At this point the objectives can be considered met, though it should be noted that the current level of risk is relatively **HIGH**.

Ten separate tests were conducted, covering a wide range of concerns – from the configuration of the operating system to physical security. Of the ten tests performed, *eight resulted in failure*. Although only two of the ten tests resulted in a ‘pass’, it should be noted that **almost all of these findings can be entirely addressed relatively quickly, and with little cost to the organization**.

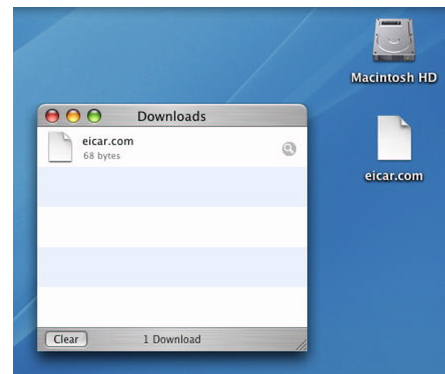
4.2 – The Findings

The following table is a summary of the tests conducted, as well as their results.

Checklist #	Item Description	Subjective / Objective	Pass / Fail
1. OSX10.3-11	Install Anti-Virus Software	Objective	Fail
2. OSX10.3-16	Disable Un-Necessary Network Services	Subjective	Pass
3. OSX10.3-13	Patch, Patch, Patch!	Objective	Fail
4. OSX10.3-2	Disable Auto-Login	Objective	Fail
5. OSX10.3-10	Home Folder Encryption	Objective	Fail
6. OSX10.3-9	Use of Strong Passwords	Subjective	Pass
7. OSX10.3-17	Enable the Firewall	Objective	Fail
8. OSX10.3-21	Open Firmware Password	Objective	Fail
9. OSX10.3-15	TCP Wrappers	Objective	Fail
10. OSX10.3-14	Central System Logs (syslog)	Objective	Fail

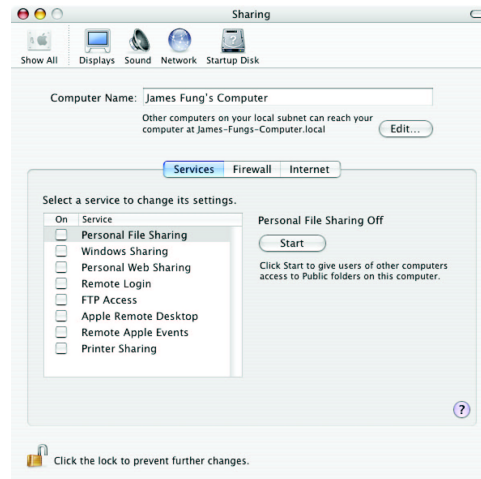
Finding Details:

- 4.2.1 Test Item #1 : OSX10.3-11 – Install Anti-Virus Software (Fail):** To test for the existence of anti-virus software, we downloaded a “test” virus to our system. This file is recognized by anti-virus software packages as a virus, but the file itself is not malicious in any way, giving us a safe and simple way of testing for anti-virus software. The image here is a scaled down version of one seen earlier, depicting the successful download of our test virus. The desired behavior would have been for an existing anti-virus software package to intercept the download and display a warning message to the user, informing them that a virus was detected and that the file had been quarantined and/or cleaned. This image shows us that the virus was not properly intercepted, meaning this system is at risk of being infected by a virus, or at the very least be at risk of being a carrier for viruses.



4.2.2 Test Item #2 : OSX10.3-16 – Disable Un-Necessary Network Services (Pass):

To confirm that our system was running only those services deemed necessary to conduct business, we used a port-scanner to check for open ports on our system. In addition, we also checked local system configuration to confirm the findings of our port scanner (see image). We are happy to report that none of the default services (web server, ftp server, remote access, etc.) were enabled. This means that the chances of this system being subject to a remote exploit of any kind via the network have been greatly reduced.



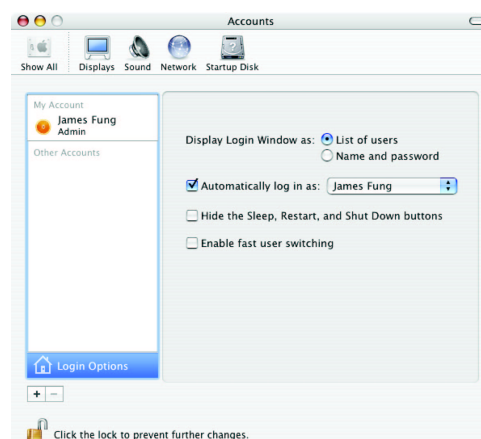
4.2.3 Test Item #3 : OSX10.3-13 – Patch, Patch, Patch! (Fail):

Applying system patches and software updates is a task found tedious by system administrators and users alike. Unfortunately, failure to apply software patches in a timely manner will give potential attackers a decided advantage and may lead to a system compromise. As seen in this image, our test system had a number of updates that have not been applied. It should be noted that not all of the updates listed here are necessarily security-related, however users should be encouraged to keep their systems up-to-date regardless.



4.2.4 Test Item #4 : OSX10.3-2 – Disable Auto-Login (Fail):

Upon booting up the system, we were immediately able to start using the system without being prompted for a single username or password. While this feature is very user-friendly and convenient for the average home user, its use should be discouraged for the corporate



user. With auto-login enabled, an attacker with physical access to the system will only have to restart the system in order to gain full access to the system's data.

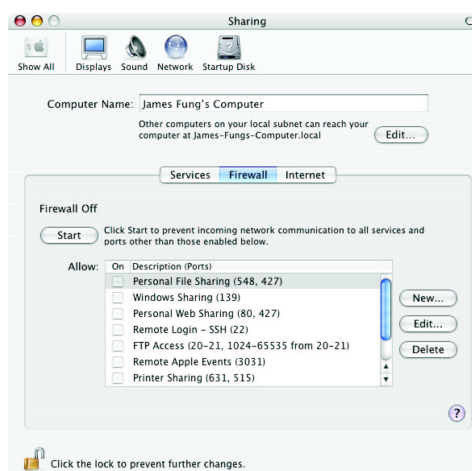
4.2.5 Test Item #5 : OSX10.3-10 – Home Folder Encryption (Fail): In the event of unauthorized physical access (a stolen laptop, for instance), it is generally only a matter of time before the intruder gains access to the data on that system. Passwords can be guessed, brute-forced, or otherwise circumvented – it all boils down to how much time the intruder has on their hands. Mac OS offers a feature called 'File Vault' which encrypts a user's home folder, where all their files are kept by default. By encrypting the home folder itself, it is no longer sufficient for an attacker to gain administrator-level access (as we were able to do). Had encryption been turned on, it could potentially take us millions of years (according to numbers published by Apple) before we were able to decrypt the contents of an encrypted folder. Instead, our test system did not have encryption enable and we were able to access the local data within minutes. Confidentiality is of the utmost importance on these systems, and FileVault should be enabled if possible.

4.2.6 Test Item #6 : OSX10.3-9 – Use of Strong Passwords (Pass): We attempted a brute-force approach to guessing the local password. Using a "dictionary" of approximately 500,000 words, our program took each word and tried to authenticate as the local user. Larger dictionaries do exist (and can be built) but were not used in this exercise due to the amount of time required. Given enough time, ALL passwords can be broken. We simply ask that users not make it too easy for intruders to guess their passwords. As hoped for, our attempts here to brute-force the password were not successful, indicating that the user's password was not one of those words in our dictionary. It is vital that users continue to choose strong passwords, as it represents the main hurdle by which intruders are kept out. Once a password is compromised, intruders are free to move about our systems with little fear of detection, as they would be entering the systems with valid, legitimate credentials.

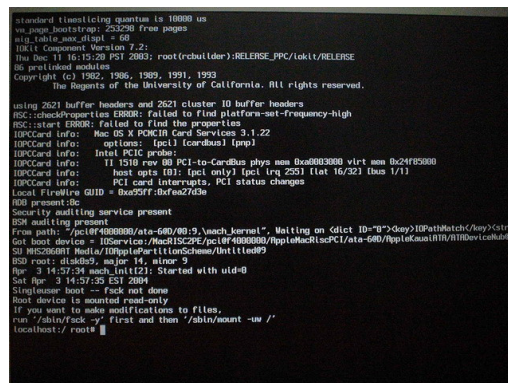


```
.....  
Password was NOT cracked!  
James-Fungs-Computer:~ jfung$
```


4.2.7 Test Item #7 : OSX10.3-17 – Enable the Firewall (Fail): We were able to confirm that the built-in firewall had not been enabled. We checked the local system configuration (image) and noted that the system itself believed the firewall was off. A port scanner was also used, to serve as confirmation that there were no firewalls active on our test system. Users are not always aware of the many ways intruders may gain access into their system without their consent. New programs may be installed that open up ports without the users' knowledge. Enabling the built-in firewall will help mitigate some of this risk, as the default behavior would be to deny access to any open ports, unless overridden by an administrative user.



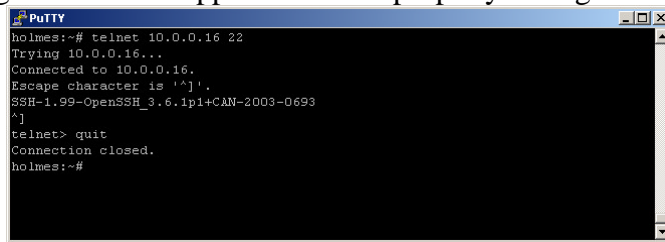
4.2.8 Test Item #8 : OSX10.3-21 – Open Firmware Password (Fail): By restarting the system and holding down specific keys on the keyboard, we were able to instantly gain administrator-level access (image). This is known as 'single-user mode', meant for use by system administrators when they need to enter the system with a minimum amount of services running – usually to recover from a failure of some kind. We were able to gain this level of access simply by holding down two keys on the keyboard, never being asked for a password of any kind. Intruders who have gained physical access will have no problems doing the same. Once they gain access to the data, they will be able to copy the data (affecting confidentiality) or worse, *change* the data (affecting integrity).



4.2.9 Test Item #9 : OSX10.3-15 – TCP Wrappers (Fail): We tested for the existence of TCP Wrappers two ways. First, we checked for the existence of the configuration files, and noted that none were found. The second test was to enable a service, and then to try and connect to that specific port (in this case, SSH (port 22)). We were able to successfully connect

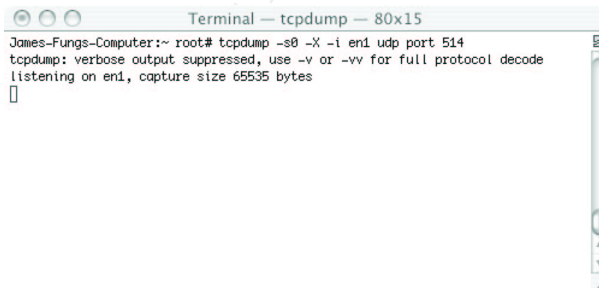
(see image), indicating that TCP Wrappers were not properly configured on our test system.

TCP Wrappers allow for an additional layer of access control and logging (defense in depth), and will be helpful both in preventing unauthorized access as well as in forensic investigations in the aftermath of a compromise.



```
holmes:~# telnet 10.0.0.16 22
Trying 10.0.0.16...
Connected to 10.0.0.16.
Escape character is '^]'.
SSH-1.99-OpenSSH_3.6.1p1+CAN-2003-0693
^]
telnet> quit
Connection closed.
holmes:~#
```

4.2.10 Test Item #10 : OSX10.3-14 – Central System Logs (syslog) (Fail): We confirmed that our test system was not sending its system logs to a central log server two separate ways: first, we checking the system configuration file (which indicated that the system was not configured to send any logs). Next, we generated our own log entries and used a network packet sniffer and performed a ‘wiretap’ on our own network connection. When we did not see the log entries leave our system, we knew that central logging was NOT configured properly. Without a proper set of logs, our forensics capability may be diminished in the event of a compromise. Should intruders manage to break in and alter the logs to hide their tracks, the lack of logs on a central server may prevent us from detecting their presence before *and* after the fact.



```
James-Fungs-Computer:~ root# tcpdump -s0 -X -i en1 udp port 514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, capture size 65535 bytes
```

4.3 – The Recommendations

The following are some recommendations to address the above findings:

4.3.1 Recommendation #1 : Modify Mac OS X Image to Reflect the Checklist.

Our test system is one of many identical systems that will end up in the hands of end users, likely with varying degrees of technical competency. That said, it is in everybody’s best interest that the system be as secure as possible by the time it makes it into the hands of the end users. For example, Anti-Virus software can be pre-installed onto the image. Network services disabled ahead of time, firewall enabled, etc. Of the ten items tested here, all but items 5 and 6 (strong password, folder encryption) can be configured prior to system delivery. **Cost:**

Approximately 8-16 hours time, at a low-level Analyst's labor grade. On-going maintenance of the image (applying new patches, updated virus signatures, etc.) will cost an additional estimated .025 FTE's (Full-Time Employee) time, averaged out over a one year period. **Compensating Controls:** If the organization cannot afford to implement this recommendation, the checklist will have to be applied by the users after they take delivery. Controls should be put in place to verify that users do indeed apply the recommended changes.

4.3.2 Recommendation #2: Publish Security Checklists to the User Community.

Users should be made aware that there is a security standard for specific types of systems (in this case OS X). The checklist used in this audit may be used as a starting point, and each division within the Laboratory can tailor it to suit their specific requirements if the need arises. The important thing is to get the checklist into the hands of the users themselves, who can help maintain the relative security levels of their systems. For example, if the users know that they have to have a screensaver password, the hope is that they will be less likely to remove the password (or the setting that enforces it) after receiving the computer. **Cost:** Approximately 40-60 hours time, at a senior-level Engineer's labor grade. On-going maintenance of the checklist will cost approximately .025 FTE's time, averaged out over a one year period. **Compensating Controls:** If the organization cannot afford to implement this recommendation, users should be referred to one of the generic checklists available (the one used in Part 2, for example).

4.3.3 Recommendation #3 : Develop a Site-Wide Policy to Enforce Standards.

Checklists and standards are only effective if users adhere to them. The Laboratory should consider a policy to enforce these standards, with appropriate penalties in the event of non-compliance. Laboratory officials will need to ensure that all employees and visitors on-site know of these new policies and have been given a fair chance to comply. **Cost:** Approximately 24 hours time, at a Security Officer's labor grade. In addition, enforcement (in the form of audits) will cost approximately .1 FTE's time at a mid-level Analyst's labor grade for the first year. After which the level of enforcement may go up or down depending on the level of cooperation on the part of the user community. **Compensating Controls:** If the organization cannot afford to implement this recommendation, efforts should be made to educate the department heads about the importance of adhering to standards. The department heads may have more success encouraging their employees to follow standards than the central IT division, especially in the absence of official policy.

4.3.4 Recommendation #4 : Purchase a Site-License for Anti-Virus Software.

Anti-Virus software is the one thing on the checklist that *will* cost additional money. To date, almost all anti-virus software licenses work on a yearly

subscription basis. Relying on users to keep their AV subscription up-to-date may end up costing the company more than it saves. The company should encourage compliance with the checklists by making the software available to all users at no extra cost to them or their departments. **Cost:** Actual cost will vary depending on vendor and number of licenses, plus additional yearly subscription and maintenance fees. **Compensating Controls:** If the organization cannot afford to implement this recommendation, consideration should be given to implementing anti-virus filtering at strategic points on the network. For example, AV software on mail servers can strip out e-mail viruses before they make it to the end users. Likewise, AV software on outbound http proxies can strip out viruses should users connect to the wrong websites.

4.3.5 **Recommendation #5 : Develop a Mandatory Security Training Program.**

Users want to do the right thing, they just don't know what the "right thing" is! Of the ten items audited in Section 3, nine were configuration settings that required no additional resources other than an educated user. In fact, the subjective items on this test (disabling un-necessary services and use of strong passwords) can really only be achieved by properly educating the users as to their significance. The training can be online or instructor-led, depending on the resources available. At the very least, it is recommended that all new-hires at the Laboratory meet with the Chief Security Officer or a member of the security team as part of human resources' orientation program. The meeting need not take long, 5-10 minutes should suffice – long enough to get acquainted and learn the basic security policies of the company. **Cost:** This recommendation will be the most costly to implement, but the organization will also stand to gain the most from a successful deployment. Approximately .5 FTE's time at a high-level professional's labor grade to develop and teach the class, which will evolve as policies do. Depending on the turnover rate at the company, new-hire interviews may take up an additional .05 FTE's time at a high-level Engineer's labor grade. **Compensating Controls:** If the organization cannot afford to implement this recommendation, alternate methods of communication should be attempted. Laboratory-wide e-mails, asking divisions to pass on information during their all-hands meetings, etc.

References :

- [1] NIST. "Risk Management Guide for Information Technology Systems", URL:
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- [2] InfoSecPedia. "CIA triad", URL:
http://www.securitygroup.org/wiki/wiki.php?title=CIA_triad
- [3] Apple Computer, Inc. "An Introduction to Mac OS X Security", URL:
<http://developer.apple.com/internet/security/securityintro.html>
- [4] Apple Computer, Inc. "Apple Security Updates", URL:
<http://docs.info.apple.com/article.html?artnum=61798>
- [5] Sourceforge.net. "CIS Benchmark for OS X", URL:
<http://sourceforge.net/projects/nitrogen>
- [6] CVE Editorial Board. "Common Vulnerabilities and Exposures", URL:
<http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mac+os+x>
- [7] LBNL. "Security Guidelines for Mac OS X Workstations", URL:
http://www.lbl.gov/ITSD/Security/systems/mac_guidelines_ws.html
- [8] SANS. "SANS InfoSec Reading Room, Mac/Apple Issues", URL:
http://www.sans.org/rr/catindex.php?cat_id=34
- [9] "Webopedia Home Page", URL:
<http://www.webopedia.com/>
- [10] Intego. "Intego Security Alert", URL:
<http://www.intego.com/news/pr40.html>
- [11] EICAR. "The Anti-Virus test file", URL:
http://www.eicar.org/anti_virus_test_file.htm
- [12] U.S. DOJ CCIPS. "Sample Network Banner Language", URL:
<http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm>
- [13] CERT. "Intruder Detection Checklist", URL:
http://www.cert.org/tech_tips/intruder_detection_checklist.html
- [14] HoneyNet Project. "Know Your Enemy: II, Tracking the blackhat's moves",
URL: <http://project.honeynet.org/papers/enemy2/>

- [15] Schneier, Bruce and Kelsey, John. "Secure Audit Logs to Support Computer Forensics", URL: <http://www.schneier.com/paper-auditlogs.html>
- [16] Mohling, Torleif. "Introduction to Syslog", URL: <http://www.cs.colorado.edu/~tor/sadocs/misc/syslog.html>
- [17] SANS. "Password Policy", URL: http://www.sans.org/resources/policies/Password_Policy.pdf
- [18] Microsoft Corporation. "Choosing a Good Password Policy", URL: <http://www.microsoft.com/technet/community/columns/5min/5min-302.msp>
- [19] Granger, Sarah. "The Simplest Security: A Guide To Better Password Practices", URL: <http://www.securityfocus.com/infocus/1537>
- [20] Apple Computer, Inc. "Sample Open Directory Overview", URL: http://developer.apple.com/documentation/Networking/Conceptual/Open_Directory/Chapter1/chapter_2_section_2.html
- [21] MacOSHints. "10.3: Make your password more secure", URL: <http://www.macoshints.com/article.php?story=20031107215426990>
- [22] Cerebus the Pope. "Compiling Crack", URL: <http://cerebus.sandiego.edu/~jerry/blog/article.php?story=20021025140240447>
- [23] Apple Computer, Inc. "Open Firmware Password 1.0.2", URL: <http://www.apple.com/support/downloads/openfirmwarepassword.html>
- [24] Venema, Wietse. "tcpdmatch man page", URL: <http://www.osxfaq.com/man/8/tcpdmatch.ws>
- [25] Venema, Wietse. "TCP Wrappers - blurb", URL: ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB
- [26] Apple Computer, Inc. "Open Source", URL: <http://www.apple.com/opensource/>
- [27] O'Reilly Media, Inc. "An Unencrypted Look at FileVault", URL: <http://www.macdevcenter.com/pub/a/mac/2003/12/19/filevault.html>
- [28] Apple Computer, Inc. "FileVault", URL: <http://www.apple.com/macosx/features/filevault/>
- [29] Blau, John. "TCP Cracks appear in Bluetooth security", URL: <http://maccentral.macworld.com/news/2004/02/11/bluetooth/>

- [30] Karg, James, et al. "Malicious Attacks of Wireless Access Points", URL:
<http://www.cs.ndsu.nodak.edu/~karg/Malicious%20Attacks%20of%20Wireless%20Access%20Points.ppt>
- [31] SecuriTeam.com. "Malicious DHCP Allows Root Compromise of Mac OS X",
URL: <http://www.securiteam.com/securitynews/6K0050A95S.html>
- [32] Miller, Todd. "Sudo Main Page", URL:
<http://www.courtesan.com/sudo/>

© SANS Institute 2004, Author retains full rights.