Mac OS X Security Assessment Project

Jeff Jones

Information Security Capstone Project – 68-595

April 2008

Mac OS X Security Assessment Project

ABSTRACT

Based on the Apple's advertisements, Mac OS X is marketed to be totally safe from viruses and spyware. This study investigated these claims to determine if there are vulnerabilities in the system. The paper provides a brief overview of the evolution of Mac OS X, a vulnerability assessment, and the identification of potential threats. The paper suggests appropriate control measures to preserve the confidentiality, integrity, and availability of the Mac OS X computing environment.

The conclusion is the Mac OS X operating system is not known to have a virus that exploits the OS. The most likely way to infect a Mac is through a web browser by using cookies and tricking the user to install malicious software. The computer may carry some form of virus or malicious software, but this does not penetrate the operating system itself. The open-source foundation of the operating system, BSD and Darwin, is very secure.

TABLE OF CONTENTS

Mac OS X Security Assessment Project

OBJECTIVES

The objectives of the Mac OS 10 Security Assessment Project are to determine if there are any vulnerabilities in this end-user computer system as packaged from Apple and identify threats and reasonable mitigation of threats. Based on some the Apple advertisements, the Mac Operating System version 10, also known as Mac OS X, is marketed to be totally safe from viruses. The common threats to typical end user systems include viruses, worms, spyware, phishing scams, trojan horses, and key loggers. In order to mitigate vulnerabilities identified, various tools and control measures are investigated.

The areas covered by this paper include a brief overview of the evolution of Mac OS X, vulnerability assessment, identification of potential threats, and appropriate control measures will be recommended to preserve the confidentiality, integrity, and availability of the Mac OS X computing environment.

INTRODUCTION

Mac Commercials

Many of the Apple commercials are available on Apple's website: http://www.apple.com/getamac/ads/

The commercials have two well known personalities, one is a PC computer, and the other is a Mac computer. Through various circumstances, the Mac plays as a superior computer system that is easier to use, bundled with all the software needed, and safer and more secure to use. Here are two quotes from these commercials.

'Viruses' commercial:

PC: Last year there are 114,000 known viruses for PCs.
Mac: PCs, not Macs.

'Trust Mac' commercial:

PC: Listen Friend, It's not very safe for me right now, you understand. There's a lot of spyware out there. Sneaks into your system... follows wherever you may go.
Mac: I run Mac OS 10 so I don't have to worry about your spyware and viruses.

Information Security

Information Security is the process of managing risks and protecting the confidentiality, integrity, and availability of information assets (data) and the related systems. Technology, administrative, and physical controls can provide adequate forms of protection from unauthorized access, use, disclosure, destruction, modification, or disruption of data .

The general purpose of information security is to ensure that the information is protected at an adequate level. Information can never be 100% protected, but there can be a high level of confidence about the security of the information.

The goals of information security are:

- ✓Protect the confidentiality and integrity of user data
- ✓Protect personal identifying information such as name and phone number
- ✓Protect data from loss

The justifications for information security are, for example:

- ✓Identity theft
- ✓Protect user's online information such as banking accounts
- ✓Prevent financial loss
- ✓Prevent loss in productivity

SECURITY ASSESSMENT

The security assessment project will analyze Mac OS X information system for potential vulnerabilities. A complete company security assessment would include a review of policies and procedures, technical assessments, risk assessments, vulnerability assessment, and threat identification. Typical end users do not have the luxury of a corporate security department with policies and procedures to protect them from the multitude of threats today. Therefore, the responsibility of information security is thrust upon the individual end user. This paper will specifically address a subset of the security assessment process by focusing on vulnerabilities of a typical end user while operating on the Mac OS X platform.

Mac OS X Evolution

The history of Mac OS 10 began in 1997 when Steve Jobs first introduced NeXT technology to Apple executives and resulted in a $427 acquisition [1]. NeXT's OPENSTEP operating system had evolved from roots of work of the Mach kernel at Carnegie Mellon University in the 1980s and later Sun Microsystems in the 1990s. Apple code named the first NeXT-based system Rhapsody and released the first developer version in September 1997 while continuing to develop and improve the existing Mac OS. The new kernel, XNU, was an integrated from Mach and BSD [2]. In 1999, the first server version of Mac OS X was released and a beta developer release called Darwin, a descendent of Rhapsody. Darwin contains hundreds of integrated software packages including the XNU Kernel, BSD, and GNU. The new Mac OS X 10 carried forward compatibility with the prior versions of Mac OS 9 by integrating Apple software APIs such as Cocoa, Classic, and Carbon. The first release of Mac OS X 10.0 was release in March 2001. As of this writing, five versions have been released:

a. 10.0 Cheetah, March 2001
b. 10.1 Puma, September 2001

c.10.2 Jaguar, August 2002
d.10.3 Panther, October 2003
e.10.4 Tiger, May 2005 (kernel Darwin 8.x)
f.10.5 Leopard, October 2007 (kernel Darwin 9.x)

Current operating system version

The current version of Mac OS X 10.5 was code-named Leopard. There are claimed to be over 300 new features since version 10.4. Software updates are digitally signed by Apple and require an administrator account and password to install. However, when moving to a new version such as 10.4 to 10.5, this is a version upgrade, or reference release, which incurs a cost associated to purchase the new version.

The Apple software is setup by default to check for updates on a regular frequency. However, care must be taken for all the third party software that would install separately from Apple's software update process? This needs to be addressed for each third party software and set to automatically check for updates. Some third party software, such as Firefox and NeoOffice, can be configured to check for it's updates automatically when the application is launched. At the moment, change to this software involve a new version release.

The Mach kernel is the lowest level of the software stack as shown in figure 1. The core of Mac OS X is built with open-source software called Darwin, an open-source operating system. Many other components of the Mac OS X are based on open-source software as well [3]. Even Safari, Mac's native web browser, uses an HTML rendering engine from the open-source community. The use of open-source software integrated into the operating system incorporates millions of developers work and time tested software to make the system free from security holes. FreeBSD Project has a Security Team that has a security auditing process facilitating a highly secure operating system by identifying and addressing vulnerabilities quickly [4]. Additionally, there is no hidden software in the code. The top layer includes native Mac system software such as Carbon and Cocoa; carried forward from the previous Mac OS 9 systems.

Figure 1: Software Stack

Security Features

The carefully integrated operating system has many features that produce an extremely secure computing platform. The core of the system utilizes open-source software that is reviewed and tested by developers all over the world. The roots of FreeBSD is a time proven secure system with the deep roots of UNIX. In fact, the Unix core is available under Apple's Open Source license which is studied by students and developers. Anyone can learn from the applications and submit suggestions and changes to code.

One of the features of a UNIX based system is the sandbox concept. A sandbox allows for application to run in a virtual container with limited access to operating system resources. Even if the process is compromised, the wider operating system cannot be exploited. In fact, there is a system library file named sandbox.h. The functionality of sandbox.h is described below by figure 2 the manual page.

SANDBOX(7) BSD Miscellaneous Information Manual SANDBOX(7)

NAME

sandbox -- overview of the sandbox facility

SYNOPSIS

#include <sandbox.h>

DESCRIPTION

The **sandbox** facility allows applications to voluntarily restrict their access to operating system resources. This safety mechanism is intended to limit potential damage in the event that a vulnerability is exploited. It is not a replacement for other operating system access controls.

New processes inherit the **sandbox** of their parent. Restrictions are generally enforced upon acquisition of operating system resources only. For example, if file system writes are restricted, an application will not be able to open(2) a file for writing. However, if the application already has a file descriptor opened for writing, it may use that file descriptor regardless of restrictions.

SEE ALSO

sandbox-exec(1), sandbox_init(3), sandbox-compilerd(8)

Mac OS X July 7, 2007 Mac OS X

Figure 2: Sandbox Man Page

A security sandbox is built into UNIX in two ways; isolating at the process level and isolating at the user level. Each process has it's own address space. A process owned by a non-root user will have limited access to root level services and files. Out-of-the-box security settings include Sudo. Sudo is utilized to prevent direct root access and mitigate access control problems. On a Mac, the root account is disabled and the administrative access is granted by use of Sudo. Sudo is a Unix command that provides a user delegated authority to execute specific commands of another user.

Standard user level security features included in Mac OS X that enhance its security include [5]:

- Access Control
- FileVault, which uses 128-bit AES encryption, optionally secures the contents of a users home directory.
- Encrypted disk images
- Key chain is a utility to manage digital certificates for email and web applications.
- Security System Preferences
- SSL/TLS secure network communication
- Kerberos authentication

Software updates can occur any day of the week, especially for critical patch releases. However, typical updates usually occur on Tuesdays and Wednesdays.

Vulnerabilities and Threats

The primary applications used for typical users include web browsing, email, and productivity applications such as word processing. According to SANS top 20 list, the number of operating system vulnerabilities is down [6]. However, application vulnerabilities is increasing. To identify the most significant vulnerabilities for a typical Mac OS X user, I performed a system vulnerability scan to discover any system issues. Following this scan, I identified the common application vulnerabilities, as well as, the typical vulnerabilities associated with any computer system such as hardware failures.

Vulnerability Scanning with Nessus

Threats originating outside of the Mac could gain privileged access through open ports on the system and exploit a vulnerability that has not been mitigated by regular software patching. To identify vulnerable ports and missing software updates, the Nessus scanning tool was utilized [7]. Before any vulnerability assessment is performed, software updates should be applied and unnecessary applications should be disabled.

The scan tool is downloaded in the standard package (PKG) format for Mac OS X. This install is simple for the client and the server. The client, for this case, is installed directly on the Mac. This allows the software to scan the installed software versions as well as ports. The Nessus scan tool is configured with plugins to determine the various tests performed. The plugin for Mac includes checks to verify that operating system and application updates have been applied. In all, the plugin includes hundreds different vulnerability checks. For example, iTunes, QuickTime, MS Office for Mac, and iPhoto are checked for security updates. Figure 3 displays the Nessus 3 installation locations.

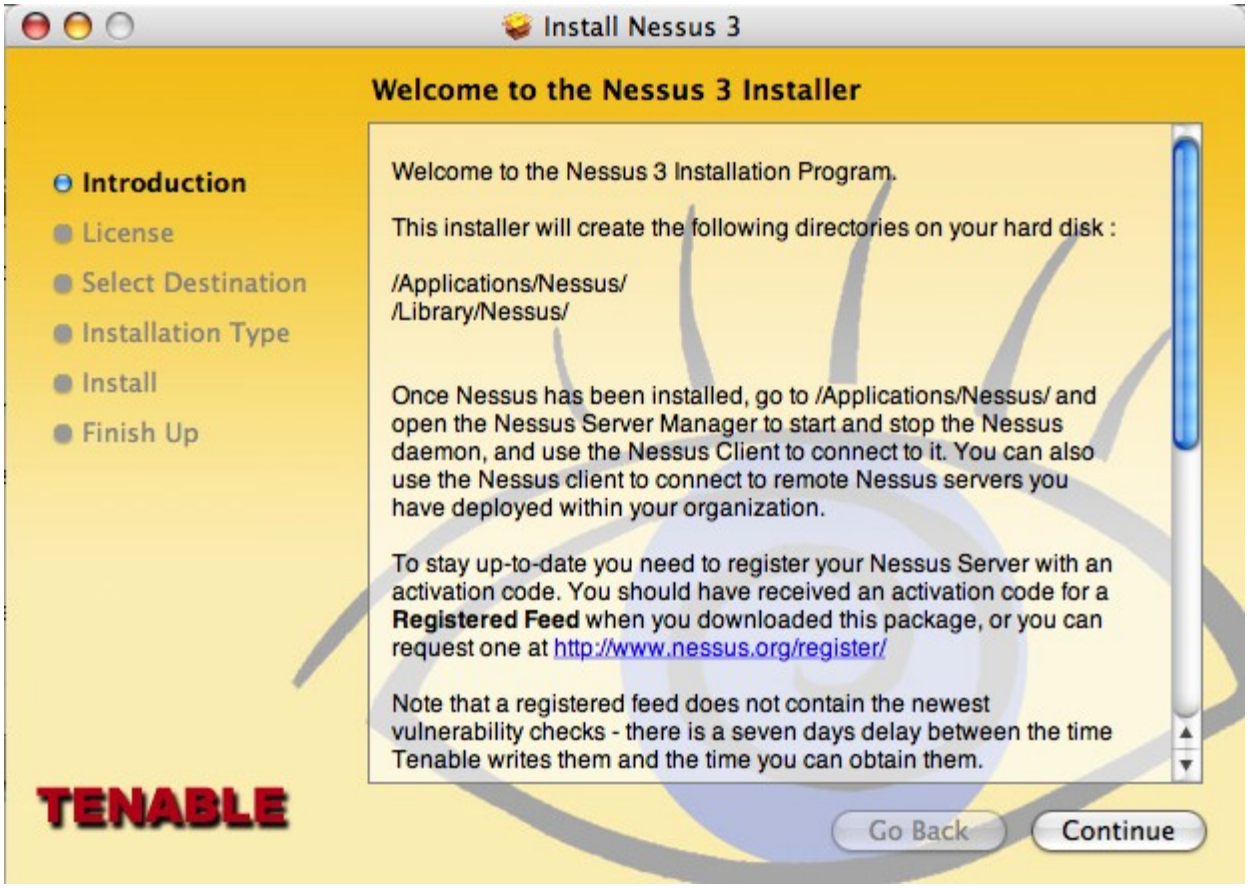

Figure 3: Nessus Install Location

The scan, displayed in Figure 4, detected five open ports on the Mac one of which (the one with the asterisk) was reported as a medium vulnerability. The full report is listed in Appendix A.

Port 1033	*NetInfo daemon
Port 1241	Nessus Server daemon
Port 661	CUPS Web server
Port 123	NPT Server
Port 6000	X Server

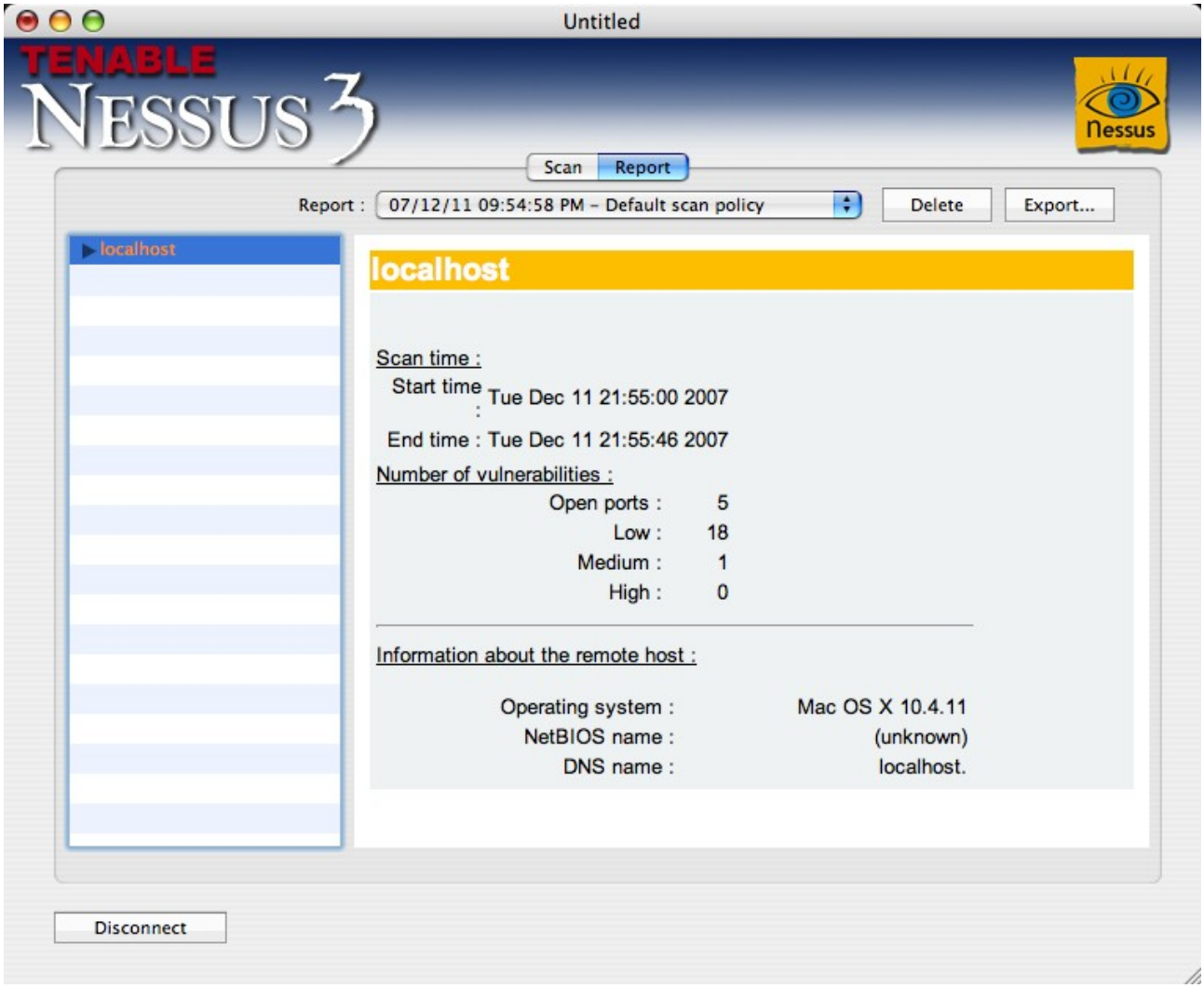

Figure 4: Nessus Scan Results

To confirm that 1033 port is open, the "netstat –an" command is run from the command line and verifies that the port is in a LISTEN state. Refer to the netstat output in Figure 5.

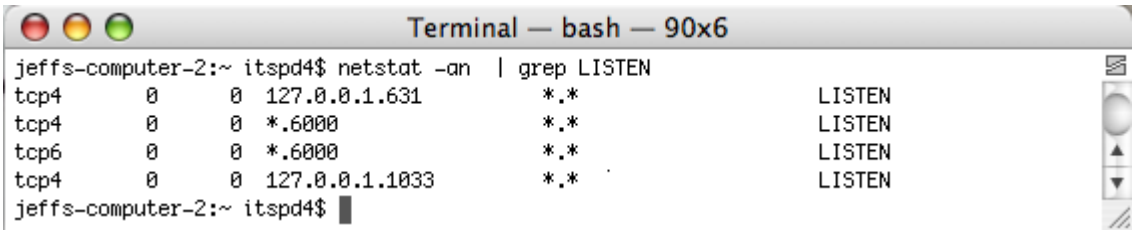

Figure 5: Netstat

The NetInfo listens on port 1033 and maintains a database including user-ids and passwords. The daemon supplies information to remote hosts on the network. In this case, the password file was retrieved (See Nessus report in Appendix A). The Nessus recommendation is

to disable this service if the host is not used in this capacity and at a minimum, the incoming traffic should be filtered by a firewall. This vulnerability allows for an attacker to use the user account information to set up a brute force attack against these user accounts.

The 18 low risk vulnerabilities are listed in Appendix A. These risks are low and simply report that there are other services running on the machine. Services such as NTP, iTunes, Ipv6, and SSL, as well as, list of software packages installed on the machine which provide an audit of installed software that could be utilized to review and compare to a company policy.

Anti-phishing Browser Detection

According to the US-CERT trend analysis from June 1, 2007, phishing accounts for 72% of the incidents reported to the US-CERT between January 1, 2007 and March 31, 2007 [8]. Since email is the most used application on the internet, this attack vector enables phishing to be one of the most significant threats today, especially against financial institutions [9].

To compare the standard web browser that is included with Mac computers, a phishing email was obtained and used to test the Safari and Firefox browsers [10,11]. The default Mac browser Safari, was compared to the well-known Firefox browser that is available for many operating systems such as Linux, Windows, and Mac. The the version of Safari tested was 3.0.4 and the version of Firefox tested was 2.0.11.

The phishing email sample in figure 6 is used for this case study and research. The page presented is pretending to be sourced by Citibank. Using a Citibank logo toward soliciting personal information under the pretext that it represents Citibank. As noted in this screen shot, a mouse-over the “Get Started” link displays the actual URL as http://skifer.as/cgi/index.html and contains no reference to Citibank. The “.as” component of this URL indicates a site in Australia.

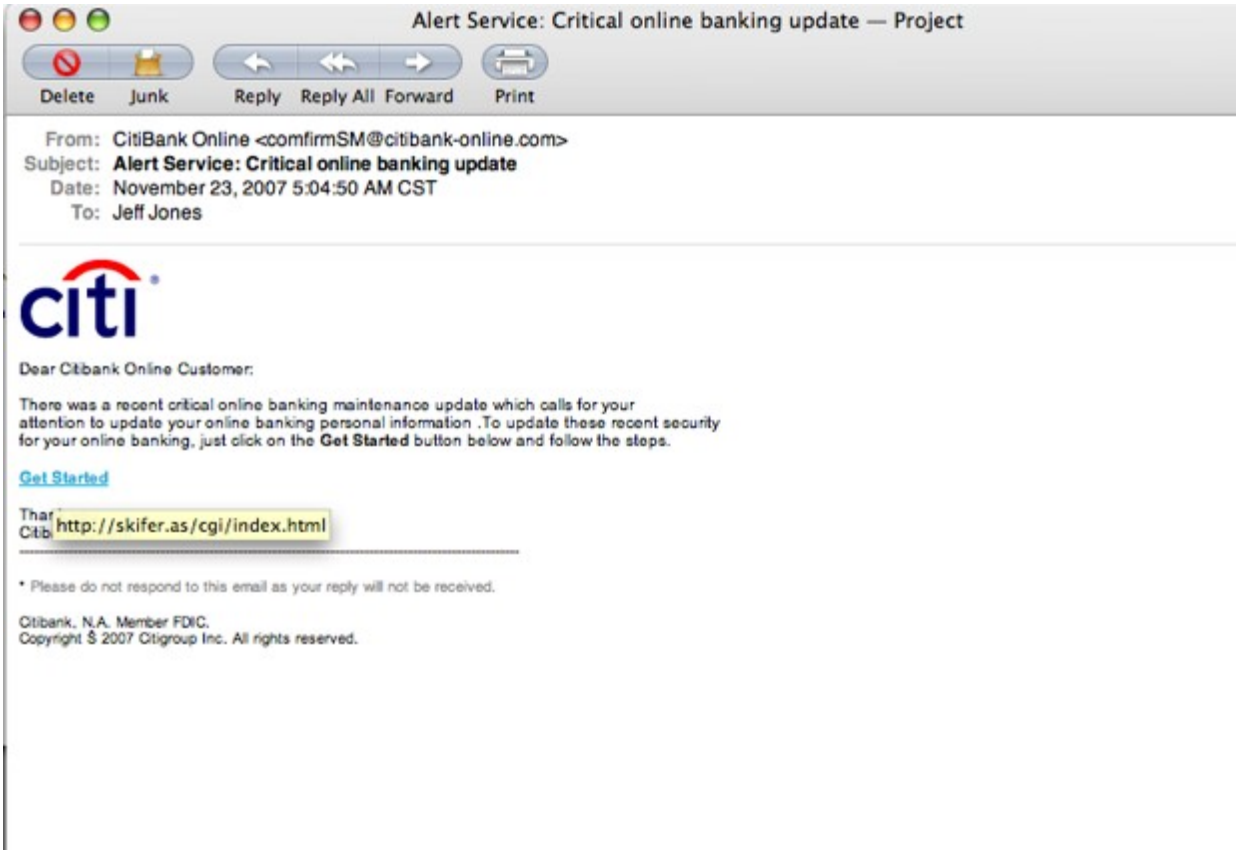

Figure 6: Phishing Sample

This skifer link is entered into the Safari browser as depicted in figure 7. The alarming result is a form to enter personal data that can be used to drain the users real Citibank account.

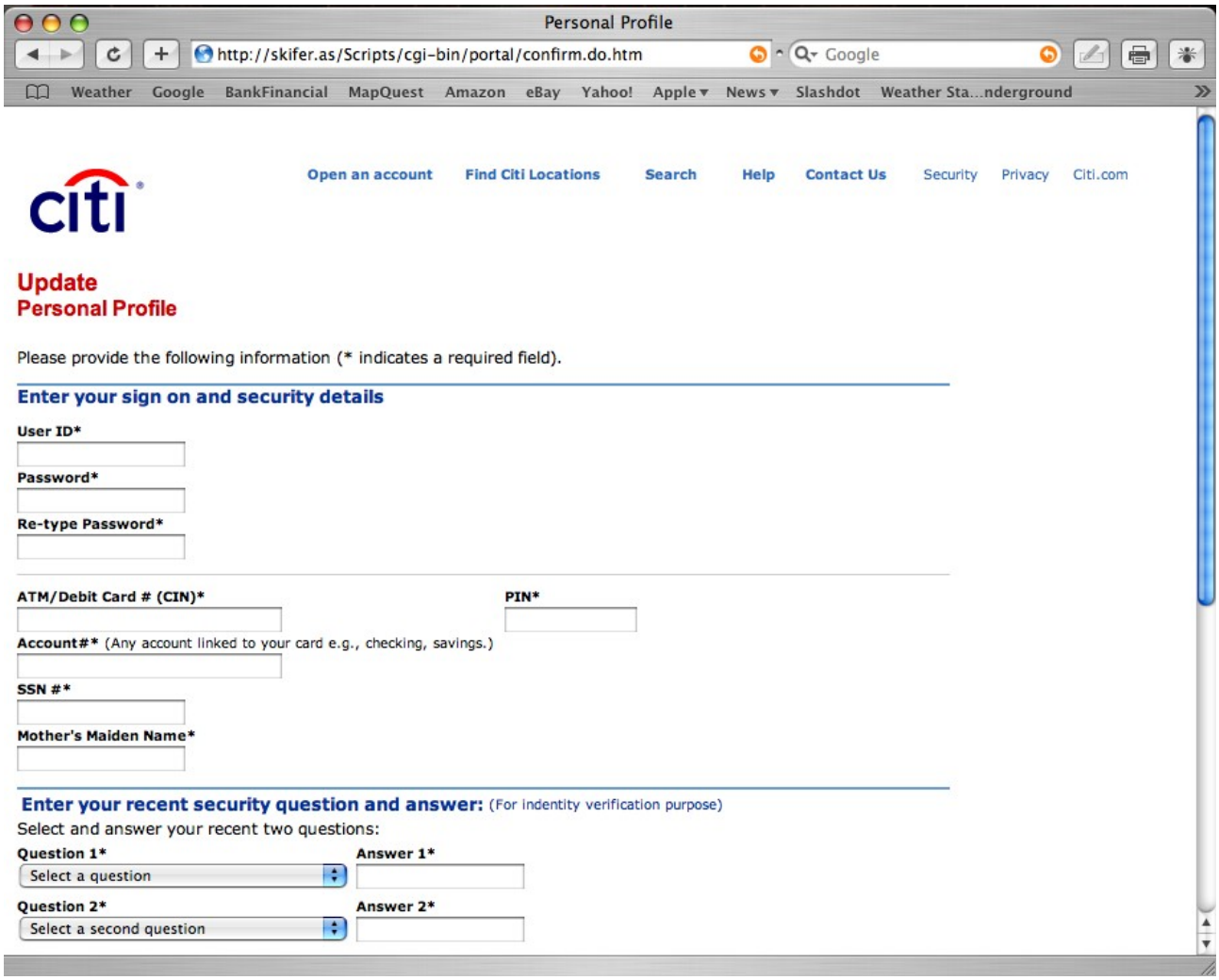

Figure 7: Safari Phishing

Next, this skifer link is entered into the Firefox browser and a phishing detection is displayed in figure 8.

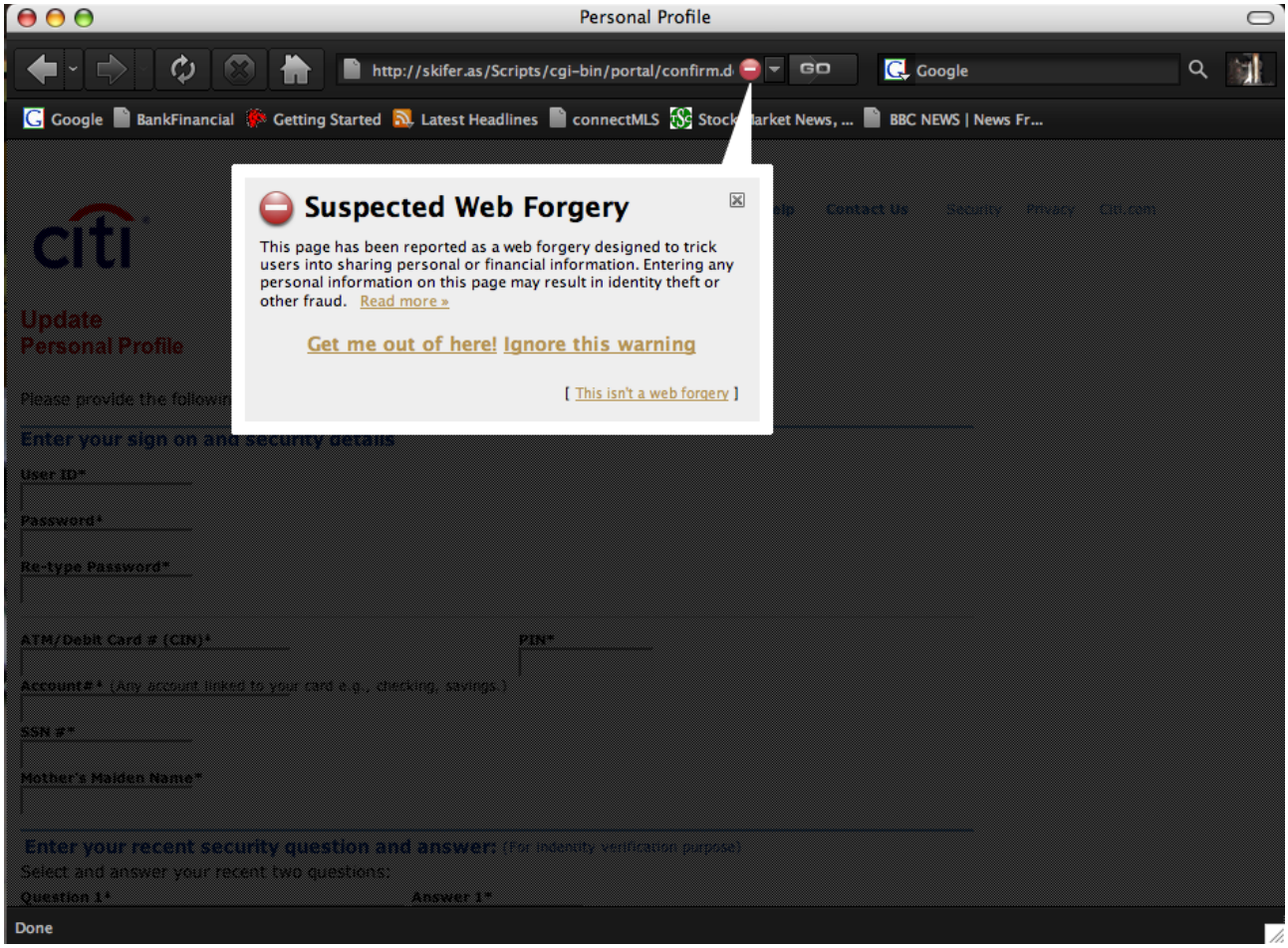

Figure 8: FireFox Phishing

The latest version of Firefox 2.x includes a new security tab with two options for detecting phishing sites. The first option checks the website with a local database of fraudulent sites and the second option will transmit the website to google for validation. However, the google validation may include sending personal information included in the URL due to the particular cookie settings of a website.

Social Engineering

Social Engineering is perhaps the most prevalent method to trick an unsuspecting or untrained user to install malicious software on their system. By using trickery, an attacker can persuade an end user to install software onto the operating system. There is very little technical mitigation to prevent this type of attack vector. The end user must be aware of such attacks and be suspicious when installing any software, especially from an Internet source. In Mac OS X, the end user is running without root level privileges. In the case where an application install is requiring elevated privileges, the user is warned that an installation is taking place and then prompted for the administrative password as displayed in figure 9 and 10.

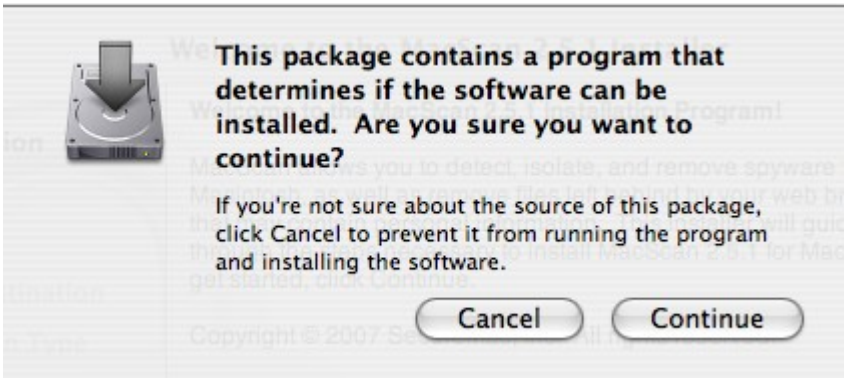

Figure 9: Prompt to run elevated

Figure 10: Prompt to enter admin password

This vulnerability is not the fault of the operating system or any application. The Trojan horse named DNSChanger (a.k.a. OXS.RSPLug.A) was an example of a social engineering attack. This Trojan Horse software could be found on 'inappropriate' web sites and would disguise as a video codec installation. This malicious software would then redirect users to other malicious web sites in order to obtain identity information.

Spyware

Spyware is one of the most hazardous tricks on the Internet. Spyware is a general term for keystroke logging, Trojan Horses, and browser session tracking via cookies. This malicious software attempts to steal personal information off of a computer system. While using a web browser, a keystroke logger or Trojan Horse could be downloaded an installed. Mac OS X provides security mechanisms that will prompt the user with warning messages prior to any installation, just like in social engineering. However, Cookies are utilized by legitimate web sites to create session variables such as shopping carts. Cookies in and of themselves, are not malicious spyware. Unfortunately, this robust feature of the Internet HTTP protocol also makes an easy attack vector for malicious web sites. Since these cookies are created and used inside the browser application, the operating system cannot detect a malicious cookie. These cookies may contain security information such as online banking session information.

Software is available to check the Mac for spyware. Downloadable from Apple's website, this software can scan the hard disk for spyware and tracking cookies. MacScan is a simple program used for scanning and cleaning up various web browser sessions. MacScan supports FireFox, Safari, Internet Explorer, Opera, and others. The tool doesn't run in realtime mode so there is no impact on performance other than when the scan is executing. According to MacScan support, cookies on the tracking cookie blacklist come from sites known to serve advertisements, spyware, malware, or track web surfing statistics. The blacklist is updated monthly to ensure accuracy and to keep the list up to date.

Installing and executing MacScan 2.5.1

Download the demo software installation package from the website to the desktop. Note the warning messages from the operating system in figure 11.

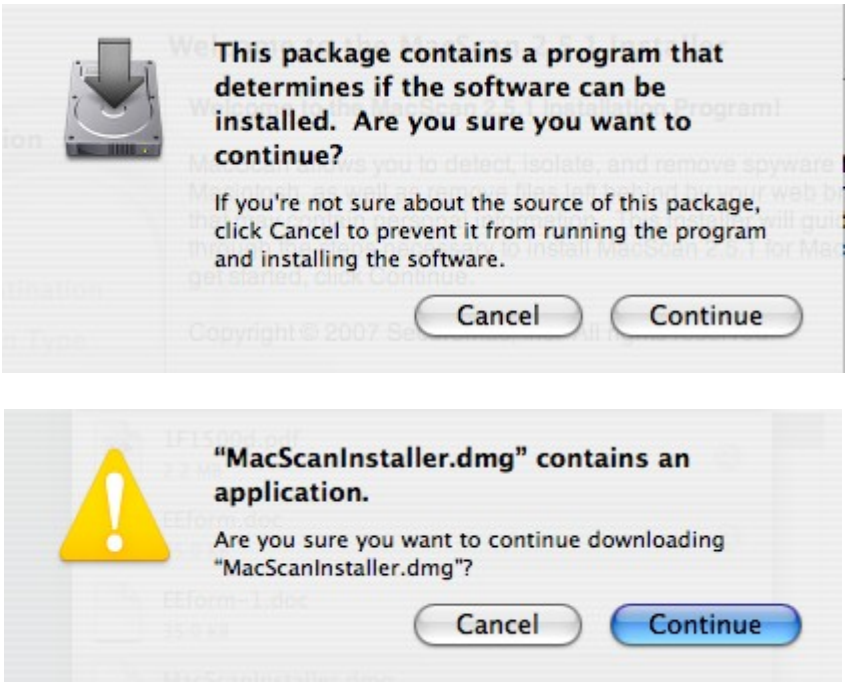

Figure 11: Download MacScan

The dmg file is saved on the desktop. DMG file type is Apple's standard install package which is similar to an ISO image. Double clicking on the icon mounts the installer package. Note that in the properties of the package the file date is Nov 19, 2007 in figure 12, therefore, the signature updates will need to be checked before scanning.

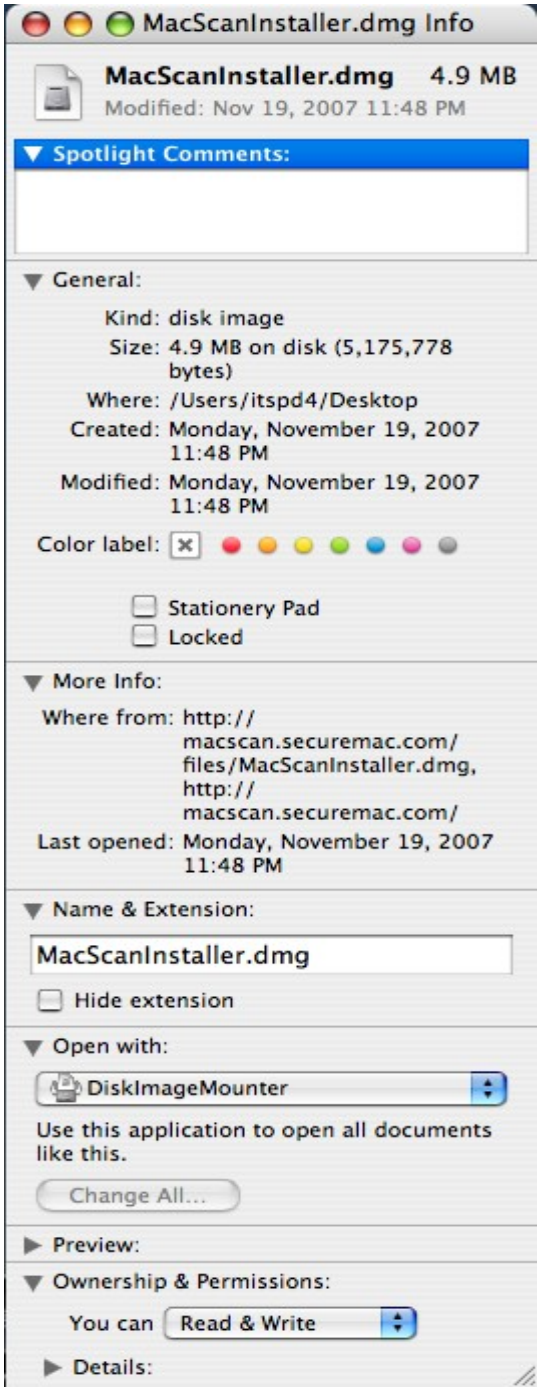

Figure 12: MacScanInstaller.dmg

As shown on the left in figure 13, the MacScan Installer in mounted and double clicking on the left window icon to launch the installer.

Figure 13: MacScan Installer

To install the software, privileged access is required, as shown in figure 14, to install into the shared /Applications/ directory thereby allowing all users on the system to run the scanning application in their home directories.

Figure 14: Elevated Privileged Installation

Typical installation process displayed in the screen shot of figure 15 completes and the installer is closed.

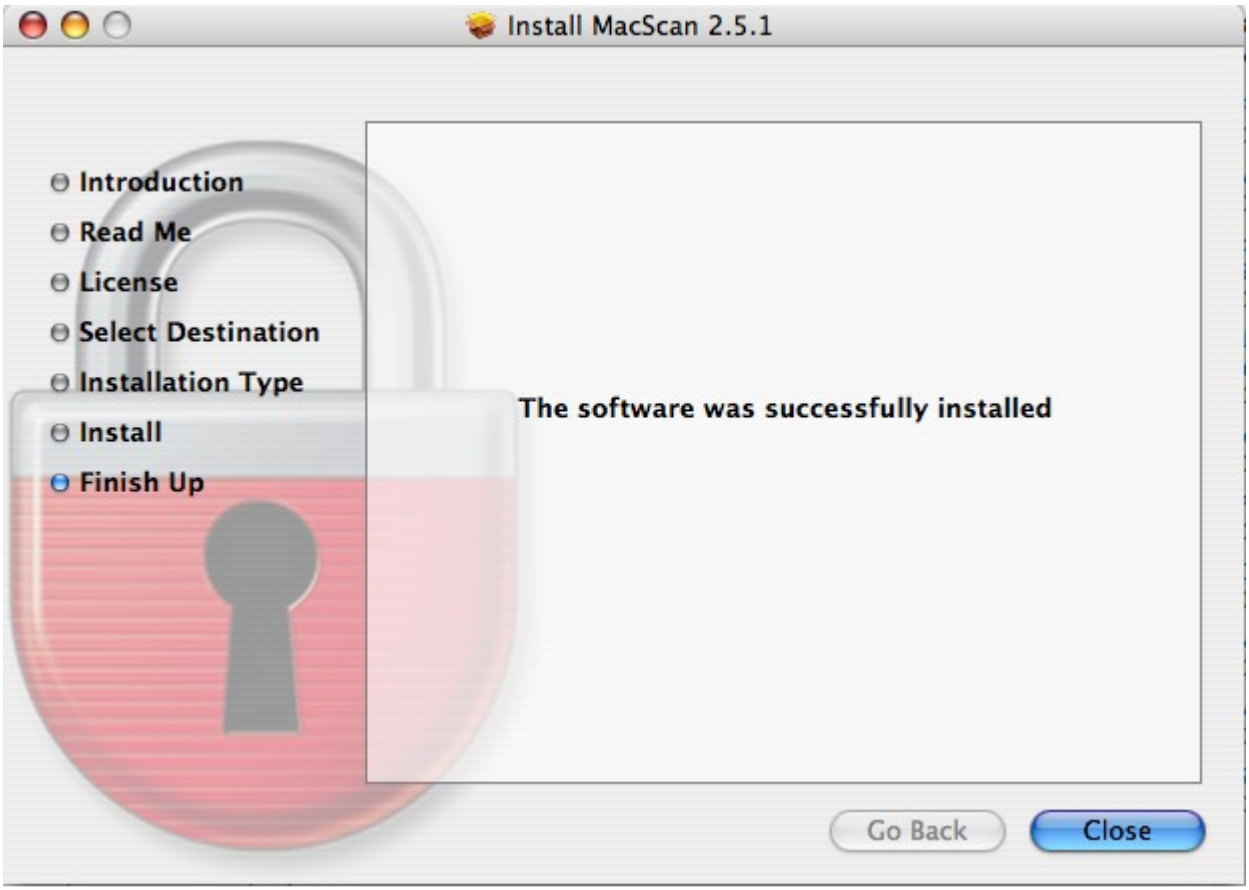

Figure 15: Installation Complete

Be sure to update the spyware and blacklisted cookie signature files. The resulting files are updated as shown in figure 16.

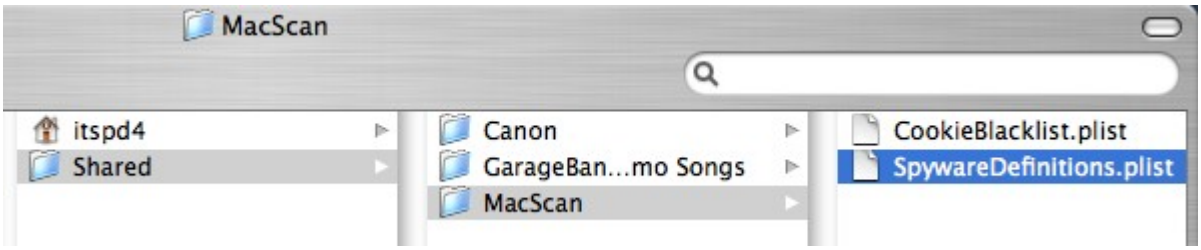

Figure 16: Update Signature Files List

Clicking on the Scan icon will perform a scan of this user's directories. The result on the sample machine displays that 32 tracking cookies were discovered. Spyware URLs are listed in Figure 17.

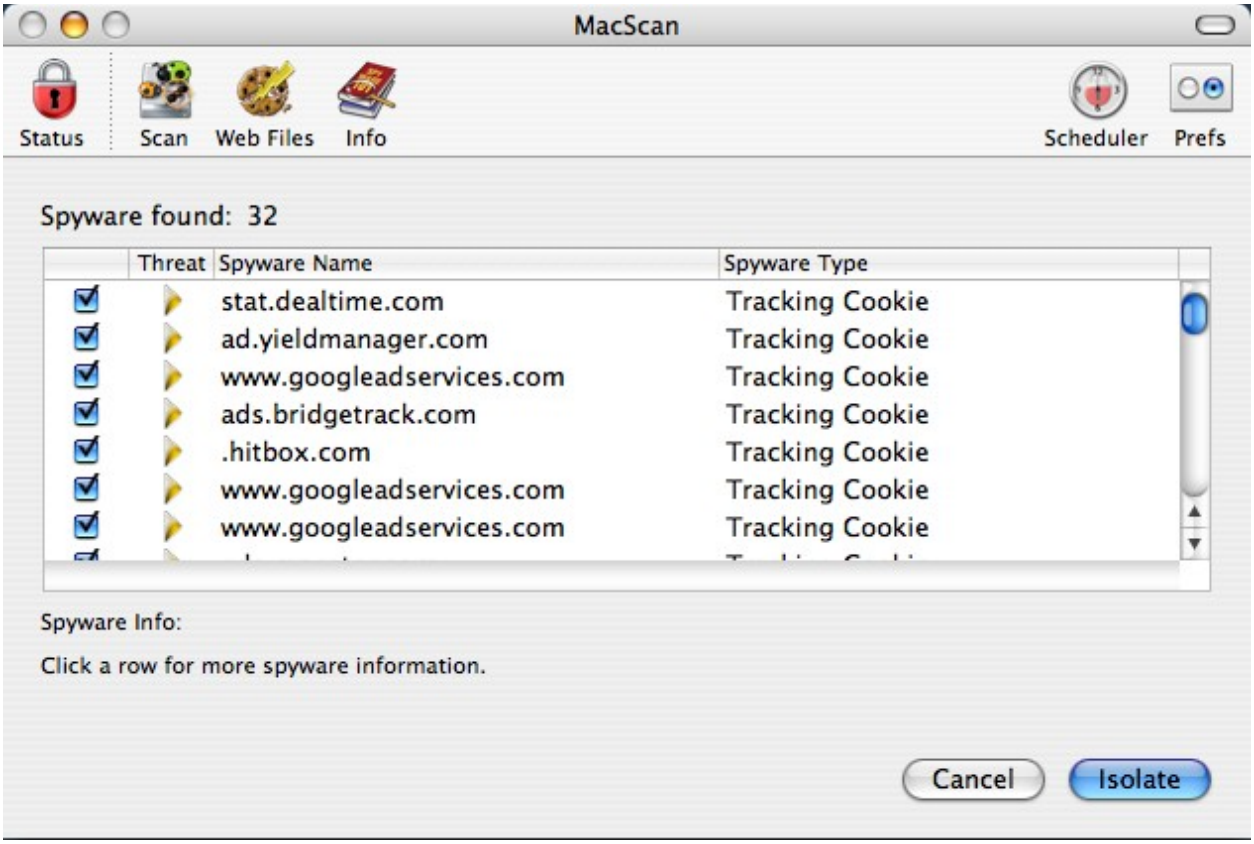

Figure 17: MacScan Results

The first scan discovers no Spyware processes (Trojans an Keyloggers), but does find 32 Tracking Cookies out of 1641 total cookies displayed in the summary screen shot in figure 18.

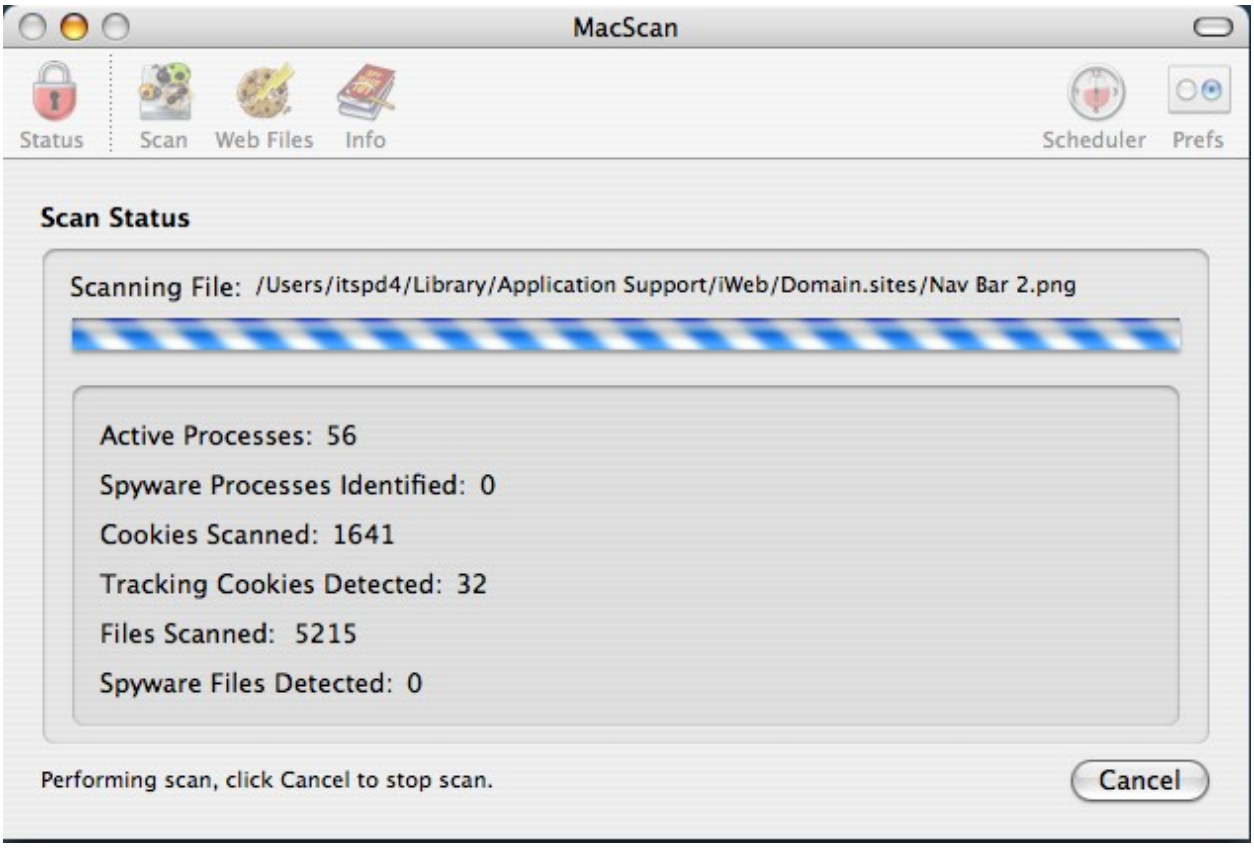

Figure 18: MacScan Results Summary

Clearing out all cookies by clicking on the “Remove Cookies” button is easily accomplished as shown below in figure 19.

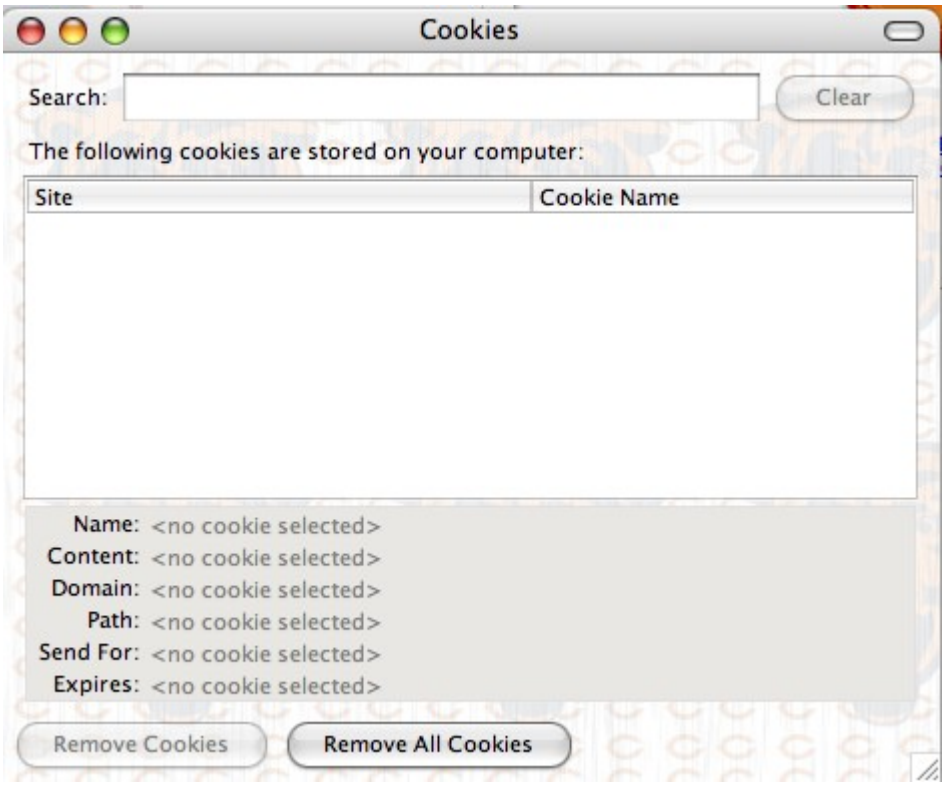

Figure 19: Remove Cookies

Rerunning the scan eliminates the “Tracking Cookies” in figure 20.

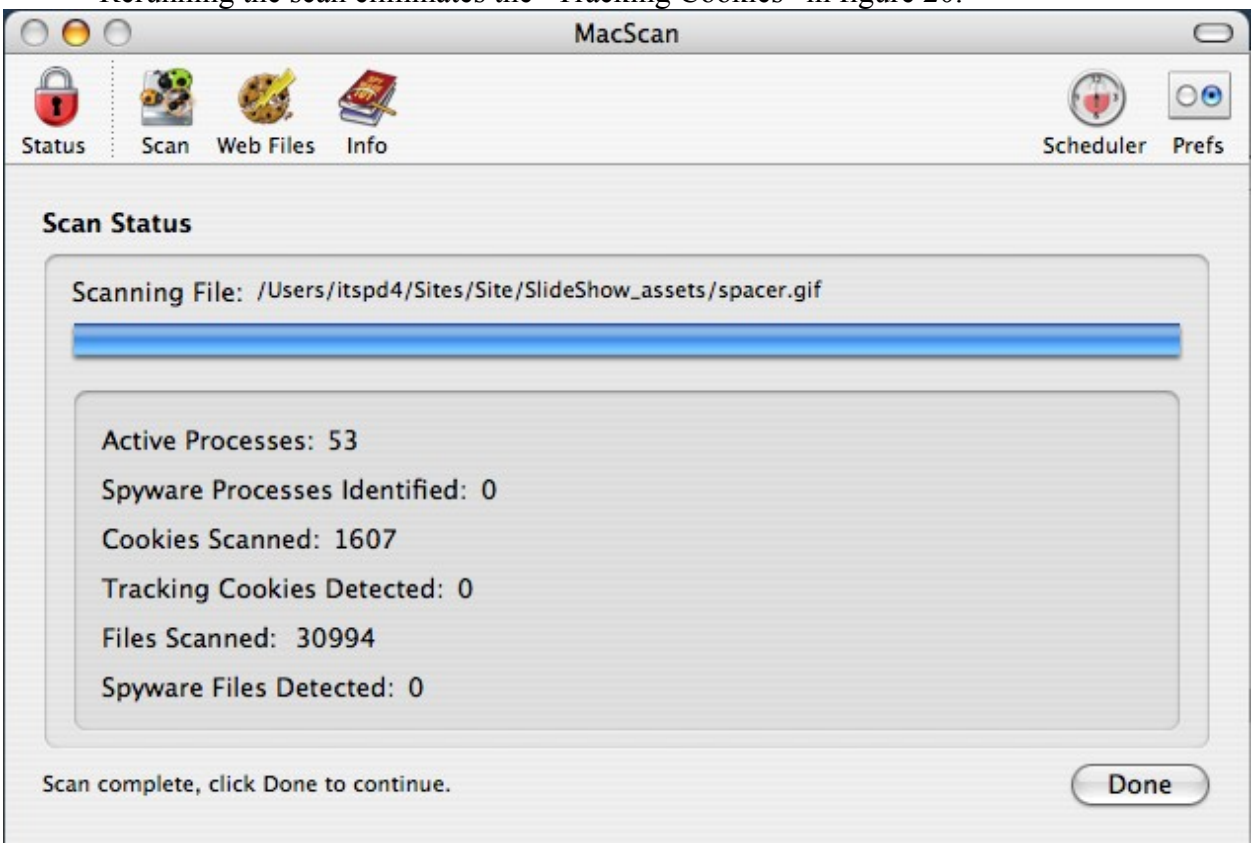

Figure 20: Rescan Results

To eliminate all cookies, simply click on the “Remove All Cookies” button. A third scan now reports zero cookies discovered displayed in figure 21.

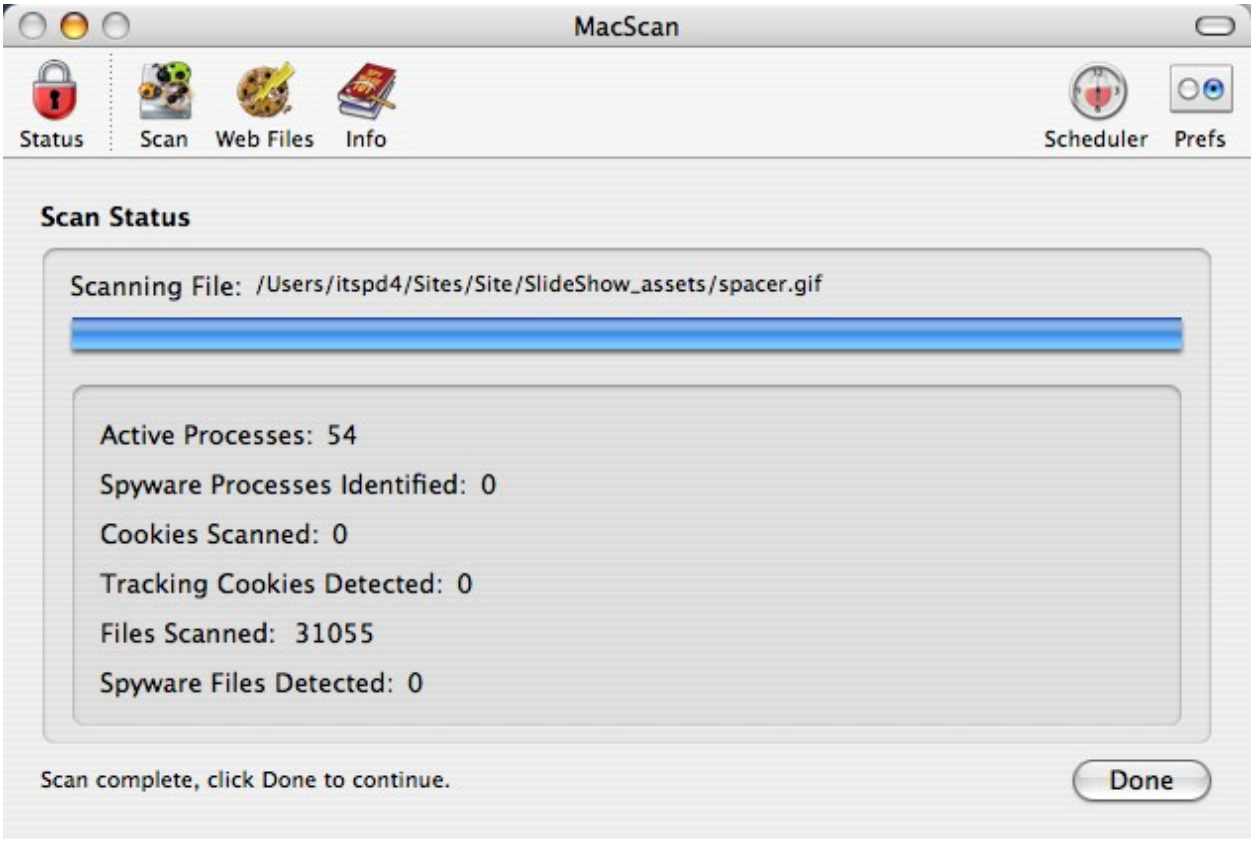

Figure 21: All Cookies Removed

FireFox cookie files are named cookies.txt and Safari cookie files are named cookies.plist. Both files are within the user directory as indicated in the file information windows in figure 22.

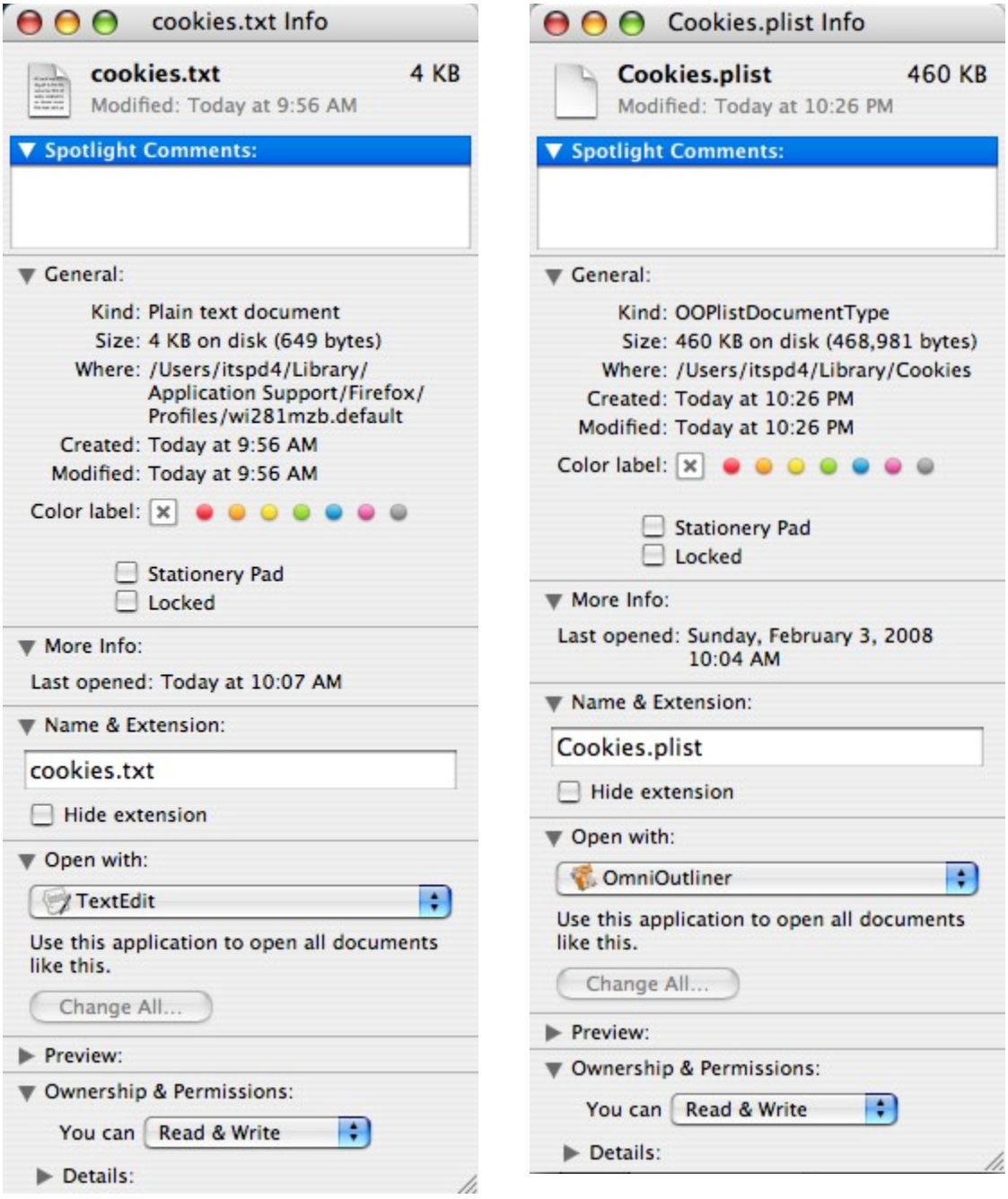

Figure 22: Cookies file locations

Virus Protection

The top ten list of viruses for December 2007 report form Sophos.com, figure 23, reports that all 10 threats are attacks against the Windows operating system [12].

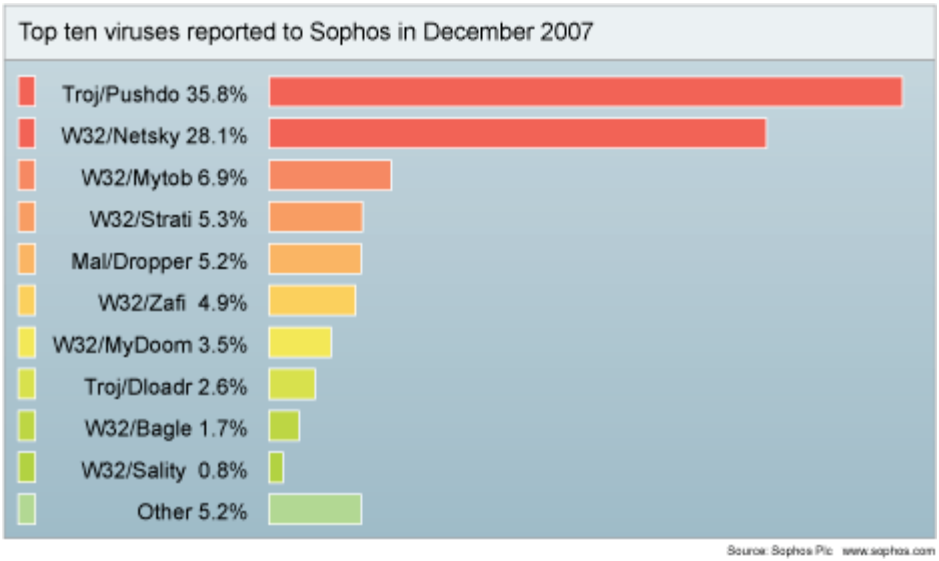

Figure 23: Sophos Top Ten List of Viruses

The advertisements for Mac OS X are typically comparisons to Windows operating systems. The primary claim is that using the default settings from the factory, Apple's Mac OS X is less prone to viruses than Windows. This leads one to believe that the system is totally secure. However, in information security, there is no such thing as 100% secure.

While investigating Apple's website, there are several pages revealed that recommend using anti-virus software. Two quotes from the Apple web site:

- Recommended maintenance activities include checking for viruses [13].

"6) Check for Viruses

Macs are far more less likely to get a computer virus like Windows PCs are prone to but that doesn't mean it's impossible. If you don't already have antivirus software, you may want to consider making a purchase. If you have the software installed, be sure to keep your virus definitions up to date—you can find the latest updates on your software manufacturer's website."

- Get a Mac; 14,000 viruses? Not on a Mac [14]

"A Mac running with factory settings will protect you from viruses much better than a PC, but it's never a bad idea to run extra virus and security software."

Anti-Virus Software for Mac OS X

Based on the information supplied by Apple's web site and the fact that no operating system is 100% secure, a search from some anti-virus software should be considered necessary. Norton Antivirus 10 for Mac is sold on Apple's web site. However, the overall customer review is 2 out of 5. It's apparent that this is a Windows PC software package hacked for Mac OS X. There are some other utilities in this package that could justify why this is needed, such as, backup and disk management functions. There is another product from Symantec called Norton Confidential for Macintosh which claims to protect against phishing web sites, secures important files and identity data, and provide early response protection against exploits discovered in applications or the OS [15].

This is an area that is not very clearly defined in the Mac universe. Most Mac users are not using virus-scanning software. The Dot-Mac online system had supplied a version of virus scanning software from McAfee named Virex. Apple mysteriously discontinued this feature of Dot-Mac and no longer provides a free virus scanner. The general consensus is that the core UNIX operating system is very secure. Windows based systems, on the other hand, have ActiveX, VBScripting, and Internet Explorer which makes them more prone to attacks. According to Todd Woodward, there are no Mac viruses, but that doesn't mean there won't be [16].

If an email contains a virus, it may be passed on to a Windows user without infecting the Mac. Another type of virus is the Word macro virus. The macro virus is launched when opening a document infected with the virus. The virus replaces the document template (.dot) and any new documents are infected with the macro virus. In the Mac OS X environment, the operating system will not be infected, but the macro virus can be embedded in documents that are passed along to other Word users. The primary method to mitigate this risk when using Word on any platform is to disable macros and force a prompt prior to running any macros.

Results - Vulnerabilities Ranking

Based on research, testing, and scanning, the results of vulnerabilities are summarized in table 1 below [17].

Prioritized Vulnerability List

Priority	Vulnerability	Instantiation Type	Threat / Trigger Source	Likelihood of Occurrence
1	**End users click on phishing link in email scam**	Accidental action	People: not understanding security, social engineering, creates opportunities for outsiders to obtain personal information	Probable
2	**End users lack training**	Accidental inaction	People: not understanding security, not disabling cookies, opportunities for session tracking	Probable
3	**End users lack training**	Combination of factors	People: not understanding security, executing files from unknown sources, creates opportunities for social engineering attack	Probable
4	**Data Loss**	Accidental inaction	System Design: System failure, loss of availability People: Fail to backup data	Occasional
5	**Unsecured server hardware**	Combination of factors	People: failure to lock laptop, creates opportunities for outsiders for theft	Probable
6	**Unencrypted sensitive files**	Accidental inaction	People: lack of understanding, failure to encrypt sensitive files, loss of confidentiality	Occasional
7	**Use of weak passwords for privileged accounts**	Combination of factors	People: not understanding security creates opportunity to obtain unauthorized access	Occasional
8	**No firewall exposes open ports**	Combination of factors	System: poor system design People: not understanding security, create opportunities for attacks, trojan horse	Occasional
9	**No Antivirus software**	Purposeful Inaction	People: Assuming there are no viruses for Mac OS X	Unlikely

Table 1: Prioritized Vulnerabilities List

PRACTICLE MAC SECURITY

Social engineering and accidental mistakes by user behavior is the highest risk to Mac OS X. Mitigating user errors and social engineering can be achieved by using the security configurations and following their advice. These essential controls provide cost effective, reasonable levels of protection for typical users. The following threat control measures provide a balance between security and consideration for user productivity.

ESSENTIAL Security

OS Update

The most important mitigation to any operating system is keeping the system patched with current software updates from the manufacturer. This screen shot displays the most frequent software update. At the minimum, a weekly updates check should be performed by configuration shown in figure 24. If installing a new system, the 'Check Now' should be performed because the install from the DVD will definitely be out of date.

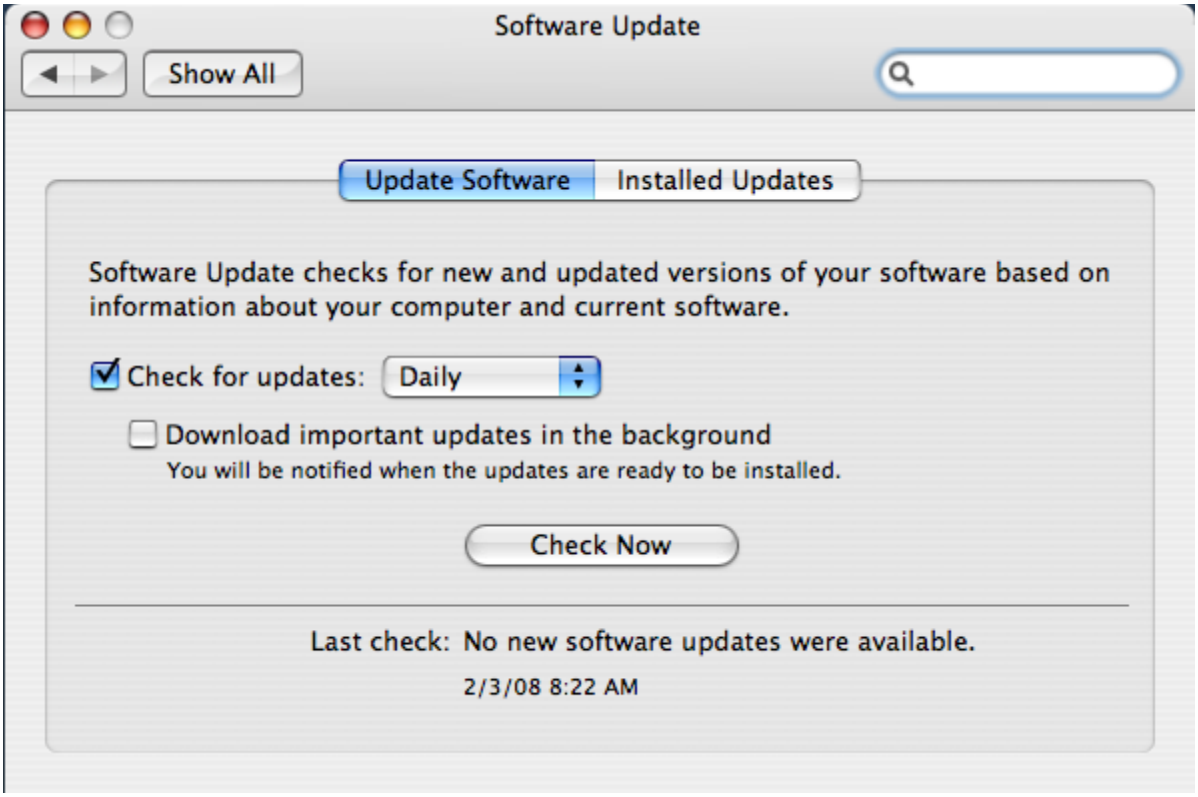

Figure 24: Software Updates

MS Word

Using Open Office, NeoOffice, or iWorks can avoid the use of Word altogether. Open Office and NeoOffice are available for free and iWorks is Apple's commercial alternative. However, if Word is absolutely needed, be sure to disable macros or only run macros only from trusted sources.

Install a Firewall

If a high speed internet connection is utilized, then a firewall/router must be installed between computer(s) and the Cable or DSL modem. If a dial-up connection is used, a system can still be attacked, just slower. Install a software firewall product on any computer that uses a dial up connection.

Email Clients

Do not use html viewing in email. Graphics can provide deceptive links to phishing sites. Always view the status bar before clicking on a link. A malicious link could be imbedded in graphics.

Use an alternate web browser

There is always a trade off when increasing security measures that effects usability. By installing and using a web browser that isn't tied to the operating system, many vulnerabilities can be eliminated. As Internet Explorer is coupled with Windows operating systems, and Safari accompanied with Mac OS X, using Firefox for web surfing can provide an additional level of security. However, IE-specific features such as proprietary DHTML, VBScript, and ActiveX are not supported in Firefox. This is good and bad in that many vulnerabilities are eliminated by not using Internet Explorer, yet some web sites require Internet Explorer's extended rich programming features.

An example of a vulnerability related to extended features is this US-CERT vulnerability as described on this site: http://www.kb.cert.org/vuls/id/998297

Firefox Security

When using Firefox or any web browser, check the privacy settings and specifically the cookie settings. The settings can help control what surfing information is stored within the browser. This is completely separate from any operating system settings. The bottom 2 check boxes will allow various types of stored information to be erased at various times.

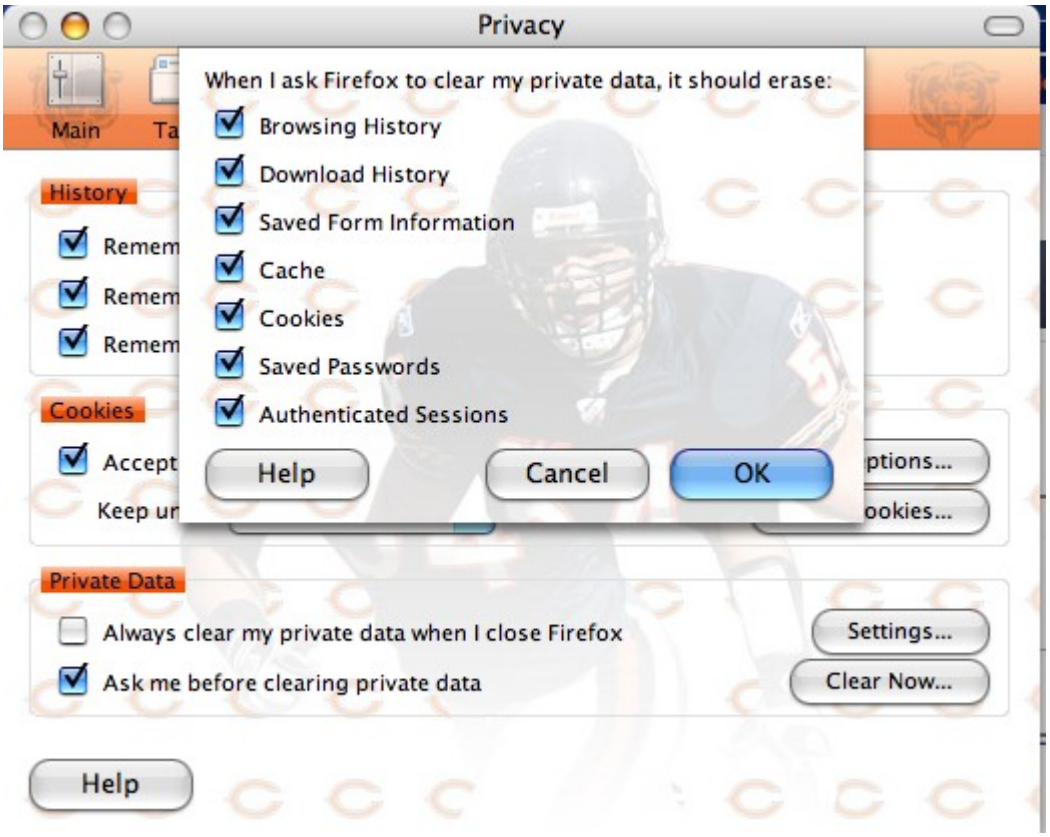

Figure 25: FireFox Security Settings

Browser Update

When using an alternate web browser, as with any application not supplied with the operating system, the application needs to be updated periodically. In Firefox, this is done in the following setup window under Tools -> Options:

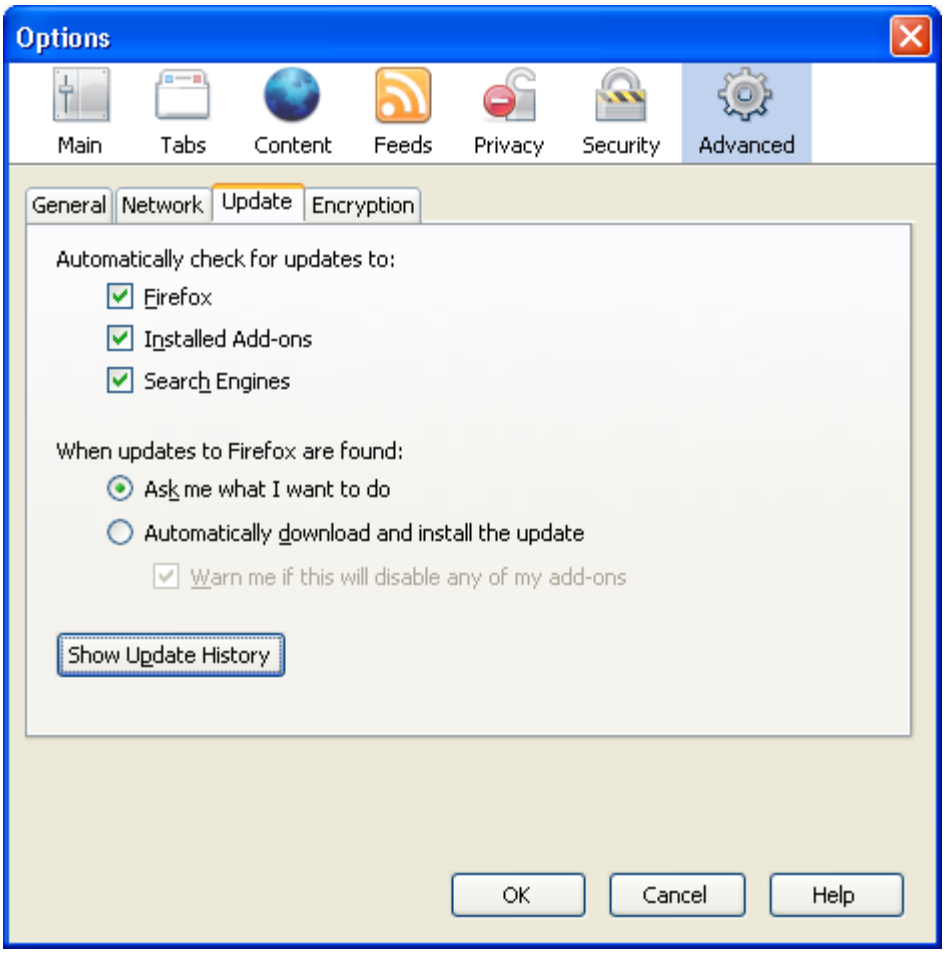

Figure 26: FireFox Auto Update Settings

Alternatively, Firefox can be updated manually to the latest version by using the pull-down menu; Help -> Updates -> Check Now for immediate update.

Safari Web Browsing

Safari does not include a malicious site detection feature, however, the cookie configuration settings available are quite good. In the security tab of the browser preferences, set the cookies option to “Only from sites you navigate to” as in figure 27 below. Unfortunately, Safari does not have the ability to build an 'exceptions' list to specifically allow or deny cookies base on their source address.

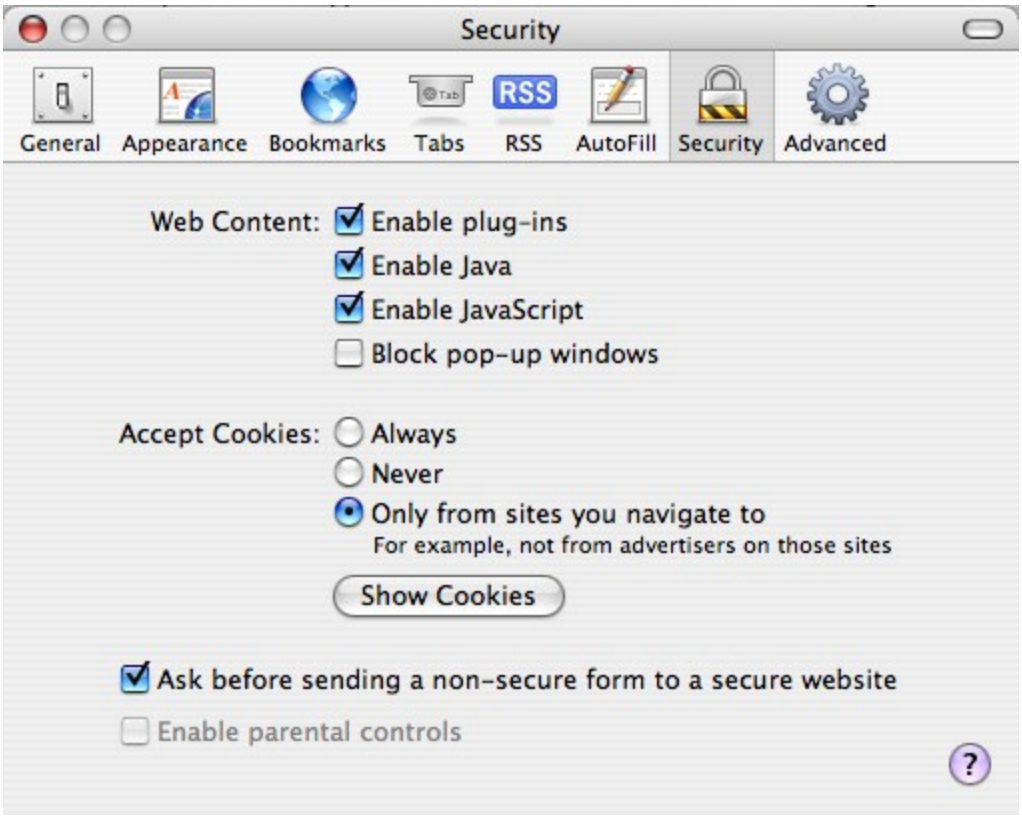

Figure 27: Safari Cookies

Clean cookies

Using a tool such as MacScan can mitigate any tracking cookies that may contain personal information from any browser in use. A weekly scan as shown in figure 28 can be setup using the scheduler feature.

Figure 28: MacScan Scheduler

ADVANCED SECURITY (mobile laptop and office use)

Away from Home

Once the computer is taking out of the home, there are many additional security concerns. From theft to unsecured wireless hotspots, additional security awareness is needed.

Disable the Automatic Login

Configure basic user account without administrative privileges and disable autologin in the System Preferences, Security window shown in figure 29. Additionally, the screen saver password may also be enabled. FileVault is an encryption setting to allow a specific user account to encrypt it's home directory [18].

Secure Important Files

Encrypting files for added security can be done easily with the built in feature of Mac OS using File Vault configuration as in figure 29. This feature will encrypt an entire user directory with Advanced Encryption Standard (AES) 128 bit encryption algorithm. A separate user account should be created and used for sensitive files thus allowing a .more selective encryption of the sensitive data.

Another alternative to encrypting an entire user account is by making an encrypted volume using the Disk Utility.

Figure 29: File Vault and Auto Login

Additional tips include logging off and shut down your laptop when not in use and physically lock the laptop in a desk or with a security cable. Don't post passwords in easily discovered places and especially not stored in the laptop carrying case.

Enable Software Firewall - ipfw

The built in firewall on Mac OS X is called ipfw. This can be configured by going into System Preferences, Sharing, and selecting Firewall. Simply click on the Start button will enable the firewall and by default, all the ports are disabled.

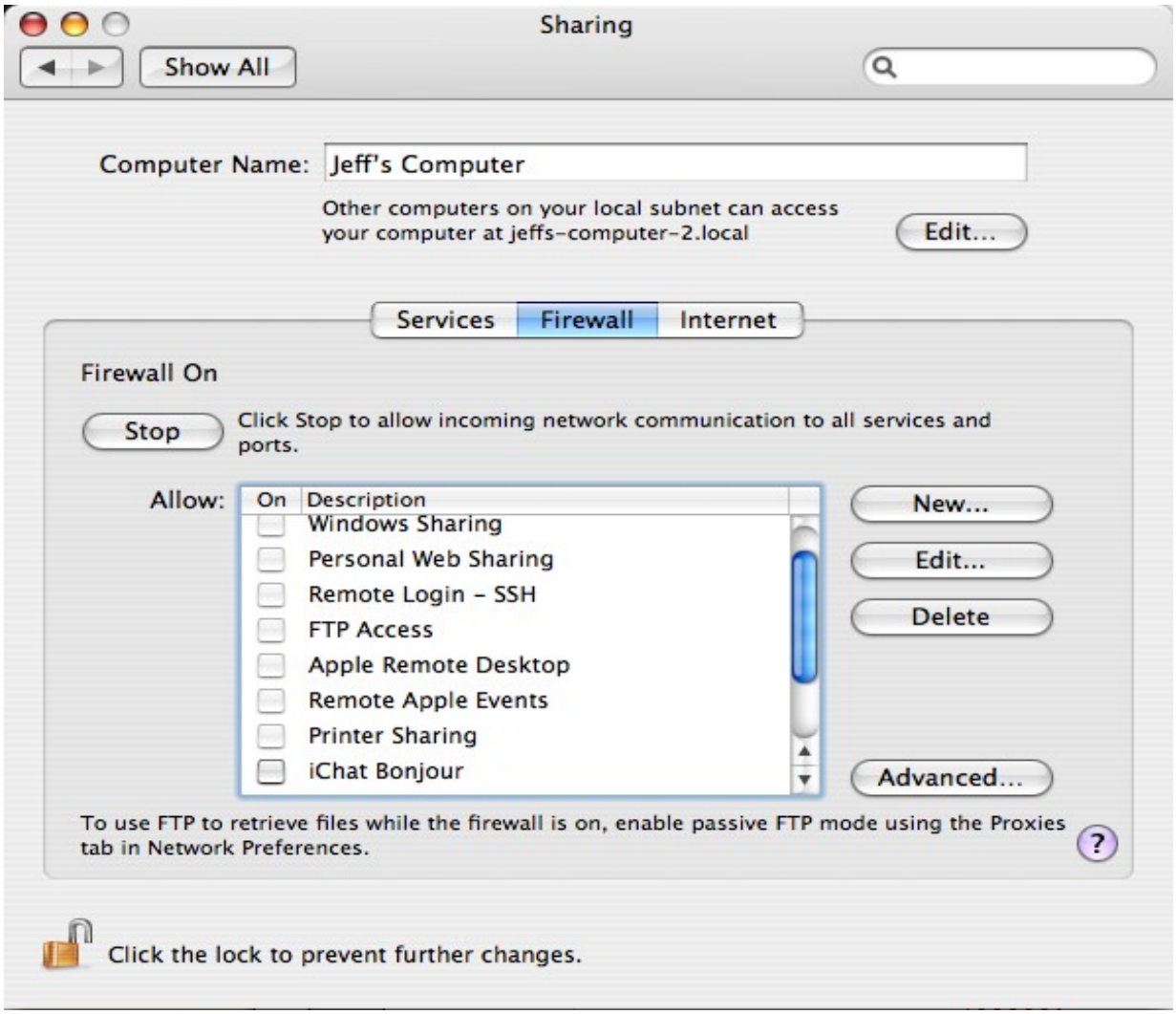

Figure 30: Firewall

Disabled ports for ssh, ftp and telnet will prevent brute force password attacks. By selecting the Advanced button, firewall logging can be enabled and track any blocked access attempts.

Figure 31: IPFW Logging

The ipfw.log file displays connection attempts that are denied. The firewall has now mitigated the medium risk level of NetInfo that was identified by Nessus. This is port 1033 and provides system information including usernames which could be used to launch a brute force password attack or other social engineering techniques. See the sample log files in figure 31.

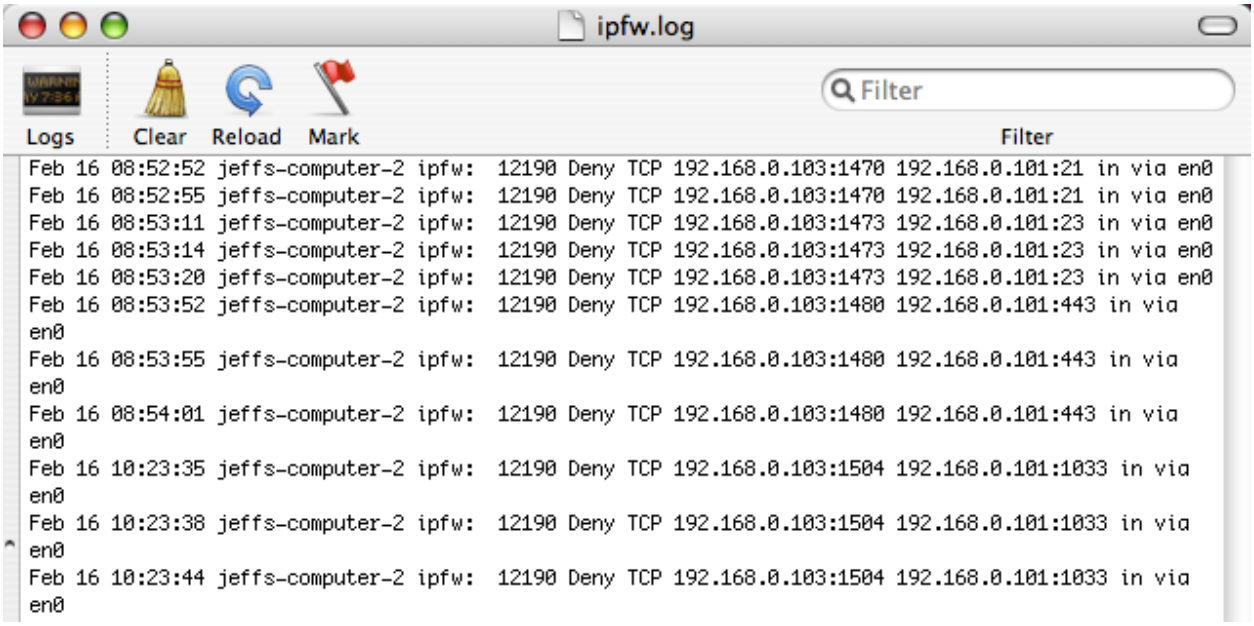

Figure 32: Firewall Deny

The firewall can also be accessed via the command line:

```
jeffs-computer-2:/etc itspd4$ sudo ipfw list
Password:
02000 allow ip from any to any via lo*
02010 deny ip from 127.0.0.0/8 to any in
02020 deny ip from any to 127.0.0.0/8 in
02030 deny ip from 224.0.0.0/3 to any in
02040 deny tcp from any to 224.0.0.0/3 in
02050 allow tcp from any to any out
02060 allow tcp from any to any established
02065 allow tcp from any to any frag
02070 allow tcp from any to any dst-port 21 in
12190 deny log tcp from any to any
65535 allow ip from any to any
```

Disable Unused Services

By default, services are disabled in Mac OS X. Be aware that any services enabled may require an additional firewall configuration to limit access. In figure 32 below, the ftp service has been enabled.

Virus Protection

Viruses, trojans, and other malware are a low risk threat to Mac OS X. Mitigating Viruses and other malware on the Mac is not relevant unless the environment is heavily integrated with Windows systems or Windows applications such as Word.

ClamXav is a free virus checker for Mac OS X with an open source engine and VirusBarrier X5 is a commercially available package [19].

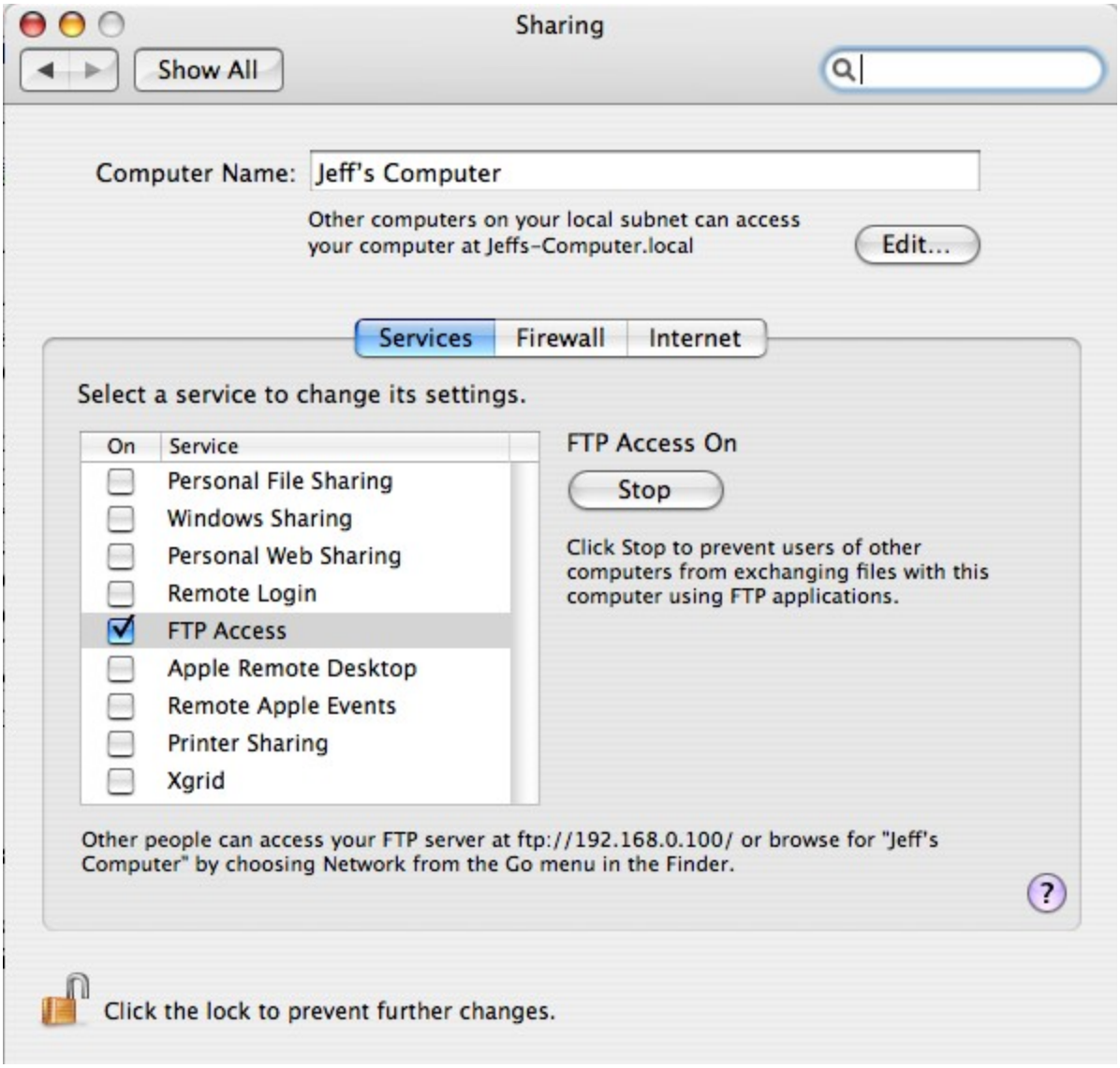

Figure 33: Enabling Service

Firmware Password

For mobile users, a firmware password should be enabled. A login password is not sufficient because there are many boot time features which allow access to the system prior to login. For example, while the system is booting, the 'T 'key can be held down to boot into Target Disk Mode that allows the firewire interface to directly access the disk. Also, the system could be booted into single user mode, boot from optical drives, and boot from the network. The firmware password will prevent this mode of operation. Details about support for firmware passwords are descripted in [20].

Cleaning Deleted Files

New in Mac OS 10.5 is a 'Secure Empty Trash' feature. In addition, there is feature to securely erase free space. This is also available in earlier versions and can be run from the Disk Utility. See figure x below.

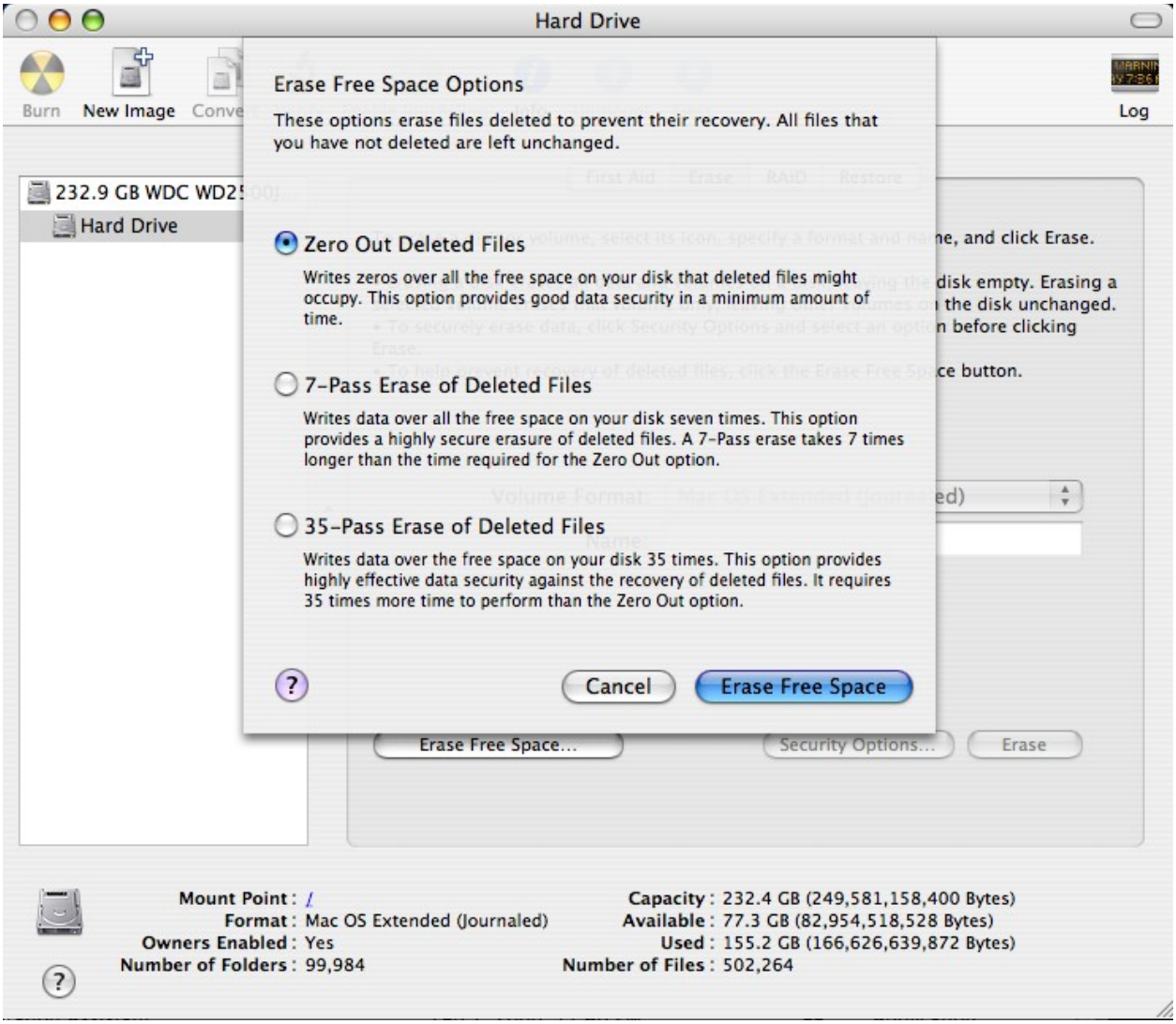

Figure 34: Secure Erase

Running Windows on Mac OS 10

There are at least two methods to install and run Windows operating systems on the Mac. One method is by booting into one operating system at a time and the other is to run a virtual Windows OS in a Mac virtual session, thus allowing for simultaneous operation.

The most recent method marketed by Apple is an application named Boot Camp. A new feature in Leopard, Boot Camp configuration partitions the hard drive and allows for only one system to be running at a given time. Either Mac OS X or Windows would be booted. With some additional software, file sharing may be achieved between the native operating systems. This method provides better performance since the Windows OS will have direct access to the

hardware such as for improved graphics performance. The Boot Camp software provides all the hardware drivers for Windows.

The second method for running Windows on a Mac is with virtualization software such as Parallels (http://www.parallels.com/). Although hardware performace is impared, this type of virtualization has many advantages. Some of the advantages are file sharing between systems, snapshots of the virtual machine for quick restoration, and support for Linux and other systems.

Unfortunately, running Windows in either configuration will expose Windows vulnerabilities the same as a standalone Windows machine. The virtualization provides better security because the virtual OS runs behind the Mac firewall. In addition, the snapshot feature provides quick backup and restoration in case of curuption.

In either case, Windows exposes the shared files to significant vulnerability. Parallels has a Security Manager feature to provide specific integration between the two operating systems. If possible, disable internet access to the Windows system should be disabled.

Password Management

Keychain is the built in Mac OS X password manager. This is accessed from the pulldown menu Applications -> Utilities -> Keychain Access. The passwords stored can be from websites and applications.

SUMMARY

The TV ads for Mac OS 10 leads one to believe that the new OS is perfectly secure and impenetrable by viruses and spyware. The study concludes that indeed, the operating system is very secure as delivered from Apple. The new Mac OS X operating system is not known to have a virus that exploits any vulnerability. The Open Source foundation of the operating system includes BSD and Darwin which is very secure.

The vulnerabilities come into play with attack vectors aimed at the applications running on the Mac. Email, Word, Boot Camp (Windows), and web browsers all in conjunction with user actions create vulnerabilities. Word can be corrupted with Word macro viruses, email can carry a virus such as a Windows virus, and web sites can utilize social engineering to trick users into executing or installing malicious software. Therefore, the computer may contain some form of malicious software, however, these changes do not penetrate the operating system itself. Particular attention should be payed to the web browser cookie settings to prevent information gathering by web sites. By configuring security settings for the operating system and applications, the Mac OS X does provide an extremely secure computing platform.

REFERENCES

[1] Singh, Amit (2004, Jan 07). A brief history of Mac OS X. Retrieved January 18, 2008, from www.kernelthread.com Web site: http://www.kernelthread.com/mac/osx/history.html

[2] Apple Inc., (2005, April 09). Sercurity_Overview.pdf. Retrieved February 2, 2008, from Apple.com Web site: http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/Security_Overview.pdf

[3] (2008). Apple - Open Source. Retrieved January 19, 2008, from Apple Web site: http://www.apple.com/opensource/

[4] (2008, March 1). FreeBSD Security Information. Retrieved March 18, 2008, from The FreeBSD Project Web site: http://www.freebsd.org/security/

[5] Apple Inc. (2005). *Mac OS X Security* (10.5 ed.), MacOSX_Leopard_Security_TB.pdf

[6] "SANS Top-20 2007 Security Risks." SANS Institue. 28 Nov 2007. SANS. 2 Mar 2008 <http://www.sans.org/top20/>.

[7] Tenable Network Security. Retrieved Dec 6, 2008, from Tenable Network Security Web site: http://www.nessus.org/nessus/

[8] (2007, June 1). Quarterly Trends and Analysis Report. Retrieved January 19, 2008, from US-CERT Web site: http://www.us-cert.gov/press_room/trendsandanalysisQ207.pdf

[9] Anti-Phishing Working Group. 2007. 25 Nov 2008 <http://www.antiphishing.org/>.

[10] "Phishing Protection." FireFox. 2006. 2 Mar 2008 <http://en-us.www.mozilla.com/en-US/firefox/phishing-protection/>.

[11] 2-FireFox Browser: http://www.mozilla.com

[12] (2007, December). Top 10 malware reported to Sophos in December 2007. Retrieved January 19, 2008, from Sophos - anti-virus and anti-spam software for businesses Web site: http://www.sophos.com/security/top-10/

[13] (2007, December 15). Mac Maintenance Quick Assist. Retrieved November 15, 2007, from Apple Web site: http://docs.info.apple.com/article.html?artnum=303602

[14] (2007). Apple - Get a Mac - Not on a Mac. Retrieved January 19, 2008, from Apple Web site: http://www.apple.com/getamac/viruses.html

[15] http://www.symantec.com/norton/theme.jsp?themeid=compchart-macintosh

[16] Woodward, Todd (2006, July 13). Mac OS X: Viruses and Security. Retrieved January 19, 2008, from Symantec Security Web site: http://www.symantec.com/enterprise/security_response/weblog/2006/07/macinenterprise_mac_os_x_virus.html

[17] Sudhanshu Kairab. A Practical Guide to Security Assessments. USA: CRC Press LLC, 2005.

[18] Reinhold, Arnold. Switching to a Mac for Dummies. Hoboken, NJ: Wiley Publishing, Inc., 2007.

[19] "VirusBarrier X5." Integro. 2 Mar 2008 <http://www.intego.com/virusbarrier/>.

[20] "Setting up firmware password protection in Mac OS X." docs.info.apple.com. 13 Nov 2007. Apple Inc.. 2 Mar 2008 <http://docs.info.apple.com/article.html?artnum=106482>

Further Technical Resources

NIST
"Computer Security Division." National Institute of Standards and Technology. 2007. 13 Nov 2007 <http://csrc.nist.gov/>.

Programming
http://gnosis.cx/publish/programming/sockets.html

Socket/Ports
http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixprggd/progcomc/skt_interf.htm

http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixprggd/progcomc/skt_ref.htm#HDRAZ4EEG34DAN

Well Known Port Numbers
http://www.iana.org/assignments/port-numbers

Nmap Scanner
http://www.insecure.org/nmap/download.html

Top Security Tools
http://www.insecure.org/tools.html

Exploits – French Security Incident Response Team

http://www.frsirt.com/

Security Conferences
http://www.blackhat.com/

Hacked websites (Note: has some graphic pictures and language)
http://attrition.org/mirror/attrition/

Benchmark/Scoring tools
http://www.cisecurity.org/

Special Interest Groups
http://www.sigsac.org/

Norton Confidential product
http://www.symantec.com/norton/theme.jsp?themeid=compchart-macintosh

Miscellaneous Links
http://www.pcworld.com/businesscenter/article/139523/article.html?tk=nl_bpxnws

http://shop.ca.com/STContent/Resources/Resources.aspx

http://security.comcast.net/get-smart/protect-your-computers/viruses-trojans-invaders.aspx

http://onguardonline.gov/index.html

http://www.sans.org/reading_room/whitepapers/sysadmin/922.php?portal=666aff97340475dec37d75ec350c03f9

http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm

Mac OS X Security Assessment Project

List of Tables

Figure Captions

APPENDIX A - Nessus Scan Report

localhost — Medium Severity problem(s) found

[^] Back

Scan time :

Start time :	Tue Dec 11 21:55:00 2007
End time :	Tue Dec 11 21:55:46 2007

Number of vulnerabilities :

Open ports :	5
Low :	18
Medium :	1
High :	0

Information about the remote host :

Operating system :	Mac OS X 10.4.11
NetBIOS name :	(unknown)
DNS name :	localhost.

[^] Back to localhost

Synopsis :

A NetInfo daemon is listening on the remote port.

Description :

A 'NetInfo' daemon is running on this port. NetInfo is in charge of maintaining databases (or 'maps') regarding the system. Such databases include the list of users, the password file, and more. If the remote host is not a NetInfo server, this service should not be reachable directly from the network.

Solution :

Filter incoming traffic to this port

Risk factor :

None

Nessus ID : 11897

Using NetInfo, it was possible to obtain the password file of the remote host
by querying it directly. The content of this file is :

. In domain 'unknown_on_port_1033' :

nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
daemon:*:1:1:System Services:/var/root:/usr/bin/false
unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false
lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
postfix:*:27:27:Postfix User:/var/spool/postfix:/usr/bin/false
www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false
eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false
sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false
cyrusimap:*:77:6:Cyrus IMAP User:/var/imap:/usr/bin/false
mailman:*:78:78:Mailman user:/var/empty:/usr/bin/false
appserver:*:79:79:Application Server:/var/empty:/usr/bin/false
clamav:*:82:82:Clamav User:/var/virusmails:/bin/tcsh
amavisd:*:83:83:Amavisd User:/var/virusmails:/bin/tcsh
jabber:*:84:84:Jabber User:/var/empty:/usr/bin/false
xgridcontroller:*:85:85:Xgrid Controller:/var/xgrid/controller:/usr/bin/false
xgridagent:*:86:86:Xgrid Agent:/var/xgrid/agent:/usr/bin/false
appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false
tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false
securityagent:*:92:92:SecurityAgent:/var/empty:/usr/bin/false
itspd4:********:501:501:Jeff:/Users/itspd4:/bin/bash

An attacker may use it to set up a brute force attack against the
remote account names.
CVE : CVE-2001-1412
BID : 2953
Other references : OSVDB:7040

Nessus ID : 11898

[^] Back to localhost

A TLSv1 server answered on this port

Nessus ID : 10330

Here is the TLSv1 server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=FR, ST=none, L=Paris, O=Nessus Users United, OU=Certification Authority for jeffs-computer.local, CN=jeffs-computer.local/emailAddress=ca@jeffs-computer.local
Validity
Not Before: Dec 12 03:39:38 2007 GMT
Not After : Dec 11 03:39:38 2008 GMT
Subject: C=FR, ST=none, L=Paris, O=Nessus Users United, OU=Server certificate for jeffs-computer.local, CN=jeffs-computer.local/emailAddress=nessusd@jeffs-computer.local
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:bc:2d:99:75:ed:3a:7d:64:00:73:d9:89:32:49:
5b:69:0a:95:c7:27:22:12:c9:ea:72:82:de:aa:da:
a1:84:2b:f3:32:1c:59:d3:39:34:95:9b:63:fd:d9:
66:6f:4b:27:91:d1:c5:eb:b9:f1:9d:ff:26:b1:9a:
ea:88:9e:66:1b:32:5b:40:24:08:6b:cd:2f:c5:28:
35:20:a6:56:5e:de:47:1b:7c:ba:4c:f1:b9:13:bf:
97:59:41:c5:21:72:2b:07:a3:6d:42:43:a6:2a:76:
14:25:e7:ab:33:f7:d8:b1:6c:c7:7e:79:06:8f:01:
e2:e4:4b:55:39:0d:dc:0b:3d
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:
71:B4:DE:14:8B:F3:68:E4:FB:E5:40:CA:15:7A:E6:12:7C:DF:B8:CC
X509v3 Authority Key Identifier:
keyid:EF:91:13:C8:77:16:0F:D5:D9:9B:3B:A3:3A:DB:77:39:95:FA:1E:7B
DirName:/C=FR/ST=none/L=Paris/O=Nessus Users United/OU=Certification Authority for jeffs-computer.local/CN=jeffs-computer.local/emailAddress=ca@jeffs-computer.local
serial:94:1F:29:E0:0E:3A:BA:BE

X509v3 Subject Alternative Name:
email:nessusd@jeffs-computer.local
X509v3 Issuer Alternative Name:
<EMPTY>

Synopsis :

The remote service encrypts communications using SSL.

Description :

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See also :

http://www.openssl.org/docs/apps/ciphers.html

Risk factor :

None

Plugin output :

Here is the list of SSL ciphers supported by the remote server :

Medium Strength Ciphers (>= 56-bit and < 112-bit key)
TLSv1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Nessus ID : 21643

Synopsis :

A Nessus daemon is listening on the remote port.

Description :

A Nessus daemon is listening on the remote port. It is not recommended to let anyone connect to this port.

Also, make sure that the remote Nessus installation has been authorized.

Solution :

Filter incoming traffic to this port.

Risk factor :

None

Nessus ID : 10147

[^] Back to localhost

A web server is running on this port

Nessus ID : 10330

Synopsis :

A web server is running on the remote host.

Description :

This plugin attempts to determine the type and the version of the remote web server.

Risk factor :

None

Plugin output :

The remote web server type is :

CUPS/1.1

Nessus ID : 10107

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Solution :

None.

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : yes
Keep-Alive : yes
Options allowed : GET, HEAD, OPTIONS, POST, PUT
Headers :

Date: Wed, 12 Dec 2007 03:55:43 GMT
Server: CUPS/1.1
Connection: Keep-Alive
Keep-Alive: timeout=60
Content-Language: en
Content-Type: text/html; charset=utf-8
Last-Modified: Sun, 25 Dec 2005 08:11:08 GMT
Content-Length: 1604

Nessus ID : 24260

[^] Back to localhost

Synopsis :

An NTP server is listening on the remote host.

Description :

An NTP (Network Time Protocol) server is listening on this port.
It provides information about the current date and time of the
remote system and may provide system information.

Risk factor :

None

Plugin output :

It was possible to gather the following information from the remote NTP host :

version='ntpd 4.2.0@1.1161-r Sun Dec 25 02:04:17 PST 2005 (1)',
processor='i386', system='Darwin/8.11.1', leap=3, stratum=16,
precision=-20, rootdelay=0.000, rootdispersion=13939.965, peer=0,
refid=STEP, reftime=0x00000000.00000000, poll=4,
clock=0xcb09da33.586c6583, state=3, offset=0.000, frequency=0.000,
jitter=0.001, stability=0.000

Nessus ID : 10884

[^] Back to localhost

Synopsis :

A X11 server is listening on the remote host

Description :

The remote host is running a X11 server. X11 is a client-server protocol which can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution :

Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:H/Au:R/C:P/A:N/I:N/B:C)

Plugin output :

X11 Version : 11.0

Nessus ID : 10407

[^] Back to localhost

127.0.0.1 resolves as localhost.

Nessus ID : 12053

Nessus can run commands on localhost to check if patches are applied
The output of "uname -a" is :
Darwin jeffs-computer.local 8.11.1 Darwin Kernel Version 8.11.1: Wed Oct 10 18:23:28 PDT 2007; root:xnu-792.25.20~1/RELEASE_I386 i386 i386

Local security checks have been enabled for this host.

Nessus ID : 12634

Synopsis :

The remote Mac OS X host has a copy of iTunes installed.

Description :

The remote host is running iTunes, a popular jukebox program.

Risk factor :

None

Plugin output :
iTunes 7.5.0 is installed on the remote host

Nessus ID : 25997

Synopsis :

This plugin enumerates IPv6 interfaces on a remote host.

Description :

By connecting to the remote Unix / Linux host with the supplied credentials, this plugin enumerates network interfaces configured with IPv6 addresses.

Solution :

Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk factor :

None

Plugin output:

The following IPv6 interfaces are set on the remote host :
- ::1 (on interface lo0)
- fe80::1 (on interface lo0)
- fe80::214:51ff:fee8:253c (on interface en1)

Nessus ID : 25202

Synopsis :

This plugin enumerates IPv4 interfaces on a remote host.

Description :

By connecting to the remote host with the supplied credentials, this
plugin enumerates network interfaces configured with IPv4 addresses.

Solution :

Disable any unused IPv4 interfaces.

Risk factor :

None

Plugin output:

The following IPv4 addresses are set on the remote host :
- 127.0.0.1 (on interface lo0)
- 192.168.0.100 (on interface en1)

Nessus ID : 25203

Synopsis :

It is possible to enumerate installed software on the remote host, via SSH.

Description :

This plugin lists the software installed on the remote host by calling the
appropriate command (rpm -qa on RPM-based Linux distributions, etc...)

Solution :

Remove software that is not compliant with your company policy.

Risk factor :

None
Plugin output:

Here is the list of packages installed on the remote Mac OS X system :
.DS_Store
.SetupRegComplete
AdditionalEssentials.pkg
AdditionalFonts.pkg
AdditionalSpeechVoices.pkg
AddressBook.pkg
AirPortExtremeUpdate2007002.pkg
AirPortExtremeUpdate2007003.pkg
AppleIntermediateCodec.pkg
AppleMobileDeviceSupport.pkg
Apple_Keyboard_Update.pkg
AsianLanguagesSupport.pkg
Automator.pkg
BSD.pkg
BaseSystem.pkg
Booth.pkg
BrazilianPortuguese.pkg
BrotherPrinterDrivers.pkg
CPU_BBBGames.pkg
CPU_ComicLife.pkg
CPU_Help.pkg
CPU_Manual.pkg
CPU_OfficeTDUS.pkg
CPU_OmniOutliner.pkg
CPU_Quicken.pkg
CPU_RegionalBoot.pkg

Remote operating system : Mac OS X 10.4.11
Confidence Level : 100
Method : uname

The remote host is running Mac OS X 10.4.11

Nessus ID : 11936

Information about this scan :

Nessus version : 3.0.6
Plugin feed version : 200712112135
Type of plugin feed : Registered (7 days delay)
Scanner IP : 127.0.0.1
Port scanner(s) : nessus_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Max hosts : 20
Max checks : 5
Scan Start Date : 2007/12/11 21:55
Scan duration : 46 sec

Nessus ID : 19506