Ethical Hacking and Countermeasures

Version 6

Module XXXIV

MAC OS X Hacking

C|EH™ Certified Ethical Hacker

News

Mac OS X hacked under 30 minutes

By Munir Kotadia, ZDNet Australia
March 06, 2006
URL:
http://www.zdnet.com.au/news/security/soa/Mac-OS-X-hacked-under-30-minutes/0,130061744,139241748,00.htm

update Gaining root access to a Mac is "easy pickings," according to an individual who won an OS X hacking challenge last month by gaining root control of a machine using an unpublished security vulnerability.

On February 22, a Sweden-based Mac enthusiast set his Mac Mini as a server and invited hackers to break through the computer's security and gain root control, which would allow the attacker to take charge of the computer and delete files and folders or install applications.

Participants were given local client access to the target computer and invited to try their luck.

Within hours of going live, the "rm-my-mac" competition was over. The challenger posted this message on his Web site: "This sucks. Six hours later this poor little Mac was owned and this page got defaced".

The hacker that won the challenge, who asked *ZDNet Australia* to identify him only as "gwerdna", said he gained root control of the Mac in less than 30 minutes.

"It probably took about 20 or 30 minutes to get root on the box. Initially I tried looking around the box for certain mis-configurations and other obvious things but then I decided to use some unpublished exploits -- of which there are a lot for Mac OS X," gwerdna told *ZDNet Australia* .

According to gwerdna, the hacked Mac could have been better protected, but it would not have stopped him because he exploited a vulnerability that has not yet been made public or patched by Apple.

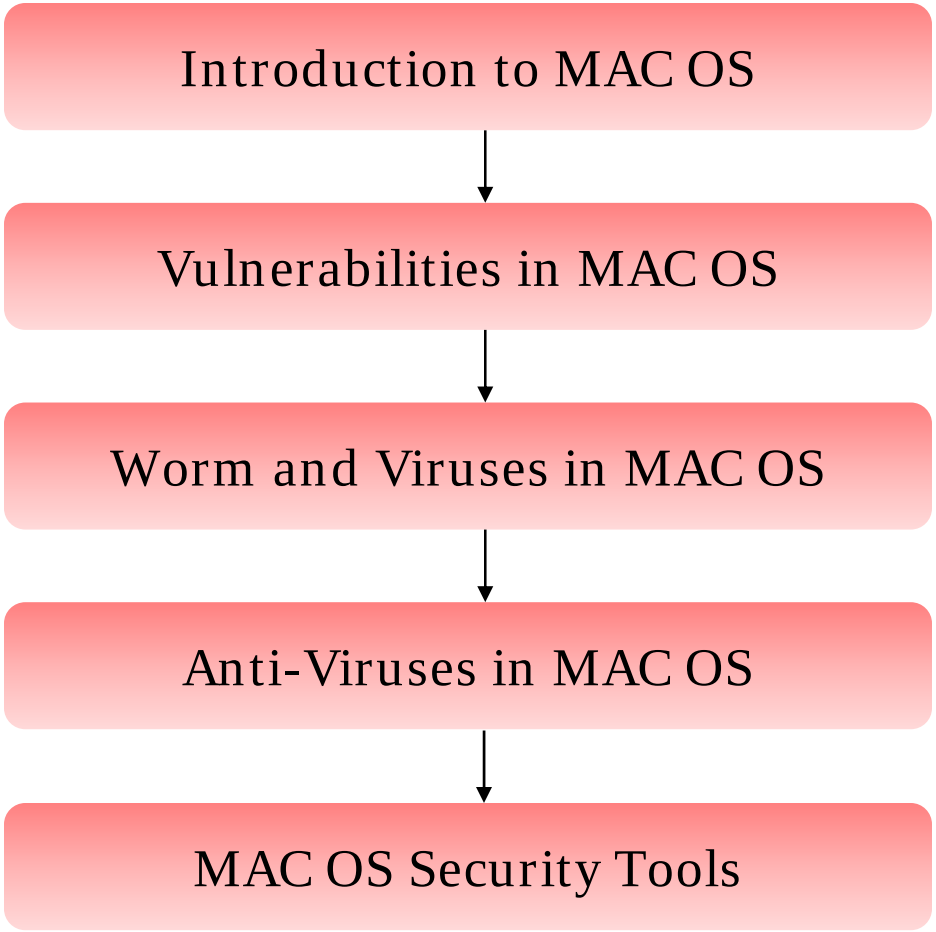
Source: *http://www.zdnet.com.au/*

Module Objective

This module will familiarize you with:

- Introduction to MAC OS
- Vulnerabilities in MAC OS
- Worm and Viruses in MAC OS
- Anti-Viruses in MAC OS
- MAC OS Security Tools

Module Flow



Introduction to MAC OS X

Mac OS X is a uniquely powerful development platform, bringing a 32-bit and 64-bit architecture and multiprocessor capability to the desktop and server arenas

It provides an extremely productive high-level programming environment, Cocoa, combined with the full power of real UNIX

Features:

- Runtime Flexibility Built on Powerful Frameworks
- Advanced Developer Tools
- Best Graphics on a Desktop
- Internationally Savvy

Vulnerabilities in MAC OS X

Crafted URL Vulnerability

Input validation issue exists in the processing of URL schemes handled by Terminal.app

By enticing a user to visit a maliciously crafted web page, an attacker may cause an application to be launched with controlled command line arguments, which may lead to arbitrary code execution

This vulnerability affects Apple Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5 and v10.5.1, and Mac OS X Server v10.5 and v10.5.1

CoreText Uninitialized Pointer Vulnerability

Apple Mac OS X CoreText is a framework for handling text on Mac OS X Tiger (10.4) and later

Mac OS X CoreText fails to properly initialize pointers, which can cause memory corruption

Any application that uses the CoreText framework for handling text is vulnerable

By convincing a user to view specially crafted text an attacker can execute arbitrary code or cause a denial of service on a vulnerable system

ImageIO Integer overflow Vulnerability

Graphics Interchange Format (GIF) is a popular image format supported by Mac OS X applications

ImageIO framework allows applications to read and write various image file formats, including GIF

An integer overflow vulnerability exists in the process of handling GIF files

By enticing a user to open a maliciously crafted image, an attacker can trigger the overflow, which may lead to an unexpected application termination or arbitrary code execution

DirectoryService Vulnerability

The Apple Mac OS X DirectoryService contains a vulnerability

This Vulnerability allows an unprivileged LDAP user to change the local root password

iChat UPnP Buffer Overflow Vulnerability

Apple iChat contains a vulnerability that could be exploited by an attacker on the local network when it attempts to handle specially crafted Universal Plug and Play (UPnP) protocol packets

A buffer overflow vulnerability exists in the UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) code used to create Port Mappings on home NAT gateways in iChat

An unauthenticated attacker on the local network may be able to execute arbitrary code or cause a denial of service

ImageIO Memory Corruption Vulnerability

The RAW Image file format is a popular image format supported by many Apple Mac OS X applications

A memory corruption issue exists in the process of handling RAW images

By enticing a user to open a maliciously-crafted image, an attacker can trigger the issue which may lead to an unexpected application termination or arbitrary code execution

A remote unauthenticated attacker may be able to execute arbitrary code or cause a denial-of-service condition

Code Execution Vulnerability

Memory corruption issue exists in Safari's handling of feed: URLs

By enticing a user to access a maliciously crafted URL, an attacker may cause an unexpected application termination or arbitrary code execution

This update addresses the issue by performing additional validation of feed: URLs and providing an error message in case of an invalid URL

A remote unauthenticated attacker who can persuade a user to click on a malicious hyperlink may be able to execute arbitrary code

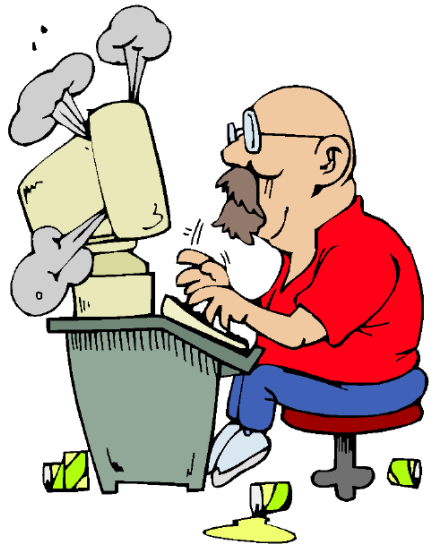
UFS Filesystem Integer Overflow Vulnerability

Unix File System (UFS) is a file system used by Unix and other similar operating systems

There is an integer overflow error in the **ffs_mountfs()** function that may occur when an OS X system opens a UFS disc image

To trigger the overflow, an attacker needs to convince a user to open a specially crafted disc image

An attacker with the ability to supply a specially crafted DMG file may be able to cause an affected system to crash, thereby creating a denial of service



Kernel "**fpathconf()**" System call Vulnerability

fpathconf() system call helps applications to find the current value of a configurable system limit

The **fpathconf()** provided with the Apple Mac OS X kernel is programmed to panic when it is passed file descriptors associated with types it cannot otherwise handle, such as semaphore descriptors returned by the **sem_open()** system call for named semaphores

This vulnerability in Mac OS X kernel could allow an authenticated local attacker to cause a denial of service

UserNotificationCenter Privilege Escalation Vulnerability

Apple's UserNotificationCenter contains a vulnerability that may allow local users to gain elevated privileges

It occurs when UserNotificationCenter runs with elevated privileges while operating on input submitted by users with normal privileges

A user with valid login credentials may be able to run commands or modify system files with elevated privileges

Other Vulnerabilities in MAC

The following is the list of some vulnerabilities in MAC that can be exploited by attacker to cause a Denial of Service:

- While decompressing malformed ZIP archives, an error exists in the "`BOMStackPop()`" function in the BOMArchiveHelper
- While processing malformed BMP images an error exists in the "`ReadBMP()`" function
- An error exists in the "`CFAllocatorAllocate()`" function when processing malformed GIF images
- Two errors exists in the "`_cg_TIFFSetField ()`" and "`PredictorVSetField()`" functions when processing malformed TIFF images

How a Malformed Installer Package Can Crack Mac OS X

An attacker can modify root-owned files, execute commands as root, by creating a malicious package and setting the authorization level to AdminAuthorization in the package

With this authorization, attacker can modify root-owned files, execute commands as root, or install setuid-root programs without alerting the user

The problem is that over 90% of Mac OS X users run as the administrator user because it is the default user created by the system

The other problem is that the package created by the RootAuthorization key as a precaution can be modified afterwards to use AdminAuthorization and can be installed without the admin's password if the account is left logged in

How a Malformed Installer Package Can Crack Mac OS X (cont'd)

When a user opens an installer package set that requires administrative privileges to install, Installer will check that the user is an administrator of the computer

Then the Installer program will run the entire install process as the root user, without prompting the user for the administrator's account password

By using this method, attacker can open a properly-formed installer package and user's system will be open to attack

Worm and Viruses in MAC OS X

Worm in MAC: OSX/ Leap-A

OSX/ Leap-A is an instant-messaging worm that attempts to spread through the iChat instant messaging system

It sends itself to available contacts on the infected users buddy list and in a file name called latestpics.tgz

OSX/ Leap-A attempts to infect recently used applications by overwriting the original application with a copy of the worm, storing the original application in the file's resource fork

Infected application files have the following extended attribute:

- Name: oompa
- Value: loompa

Inqtana.A: F-Secure Worm on OS X

OSX/ Inqtana.A is a Java based proof of concept bluetooth worm that affects only OSX 10.4 systems if they have not been patched against vulnerability CAN-2005-1333

Inqtana.A arrives to victim system as OBEX Push request, requiring user to accept the data transfer

When the transfer is done, Inqtana.A uses directory traversal exploit to copy it's files so that it starts automatically on next reboot

On rebooting, the Inqtana.A will activate and look for devices that accept OBEX Push transfers and tries to send itself to those devices

The files com.openbundle.plist and com.pwned.plist are dropped into a location from where they are called during system startup

The openbundle.plist will unpack the worm components and com.pwned.plist executes the worms

Preventive Measures for OSX Inqtana.A

OSX/ Inqtana.A affects only Mac OSX 10.4

Patch your system by getting updates from Apple

Delete the following files:

- /Users/worm-support.tgz
- /Users/InqTest.class
- /Users/com.openbundle.plist
- /Users/com.pwned.plist
- /Users/libavetanaBT.jnilib
- /Users/javax
- /Users/de
- /Users/[user name]/Library/LaunchAgents/com.pwned.plist
- /Users/[user name]/Library/LaunchAgents/com.openbundle.plist

Viruses in MAC: Macro Viruses

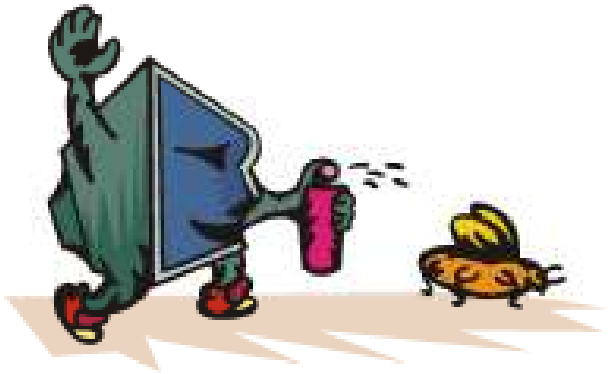
Macro viruses are the first cross-platform viruses

Most macro viruses that target Microsoft Word files, use commands such as AutoOpen, AutoClose, AutoExec, and AutoExit and copies itself into the active template, changes some menu items

When the template is edited, it changes the file types and then copies itself from the corrupted template into all new files you create or open

This virus can be removed, if caught in time, by removing the active template file, and any infected files

Other macro viruses can corrupt or delete your files, hide certain application functions, and even more



Anti-Viruses in MAC OS X

VirusBarrier

Intego VirusBarrier X4 is the non-intrusive antivirus security solution for Mac computers

It protects against viruses of all types, coming from infected files or applications, or from removable media

VirusBarrier X4 examines all the files that your computer opens and writes, as well as watching for suspicious activity that may be the sign of viruses acting on applications or other files

It works in background, detects and eradicates all known viruses including word and excel viruses, and even viruses targeting the OS

VirusBarrier: Screenshot

McAfee Virex for Macintosh

McAfee VirusScan for Mac, guards against all types of viruses and malicious code, including new and unknown threats, that target OS X

VirusScan for Mac offers unintrusive, effective protection that hunts down and kills viruses, worms, Trojans, and other malicious code as they attempt to infect systems

VirusScan automatically checks for the latest virus updates, so your protection is always up to date

McAfee Virex for Macintosh: Screenshot

Sophos Endpoint Security and Control

It provides warning of outbreak risk across the entire network with automatic email alerts and its security dashboard

Unique Behavioral Genotype Protection automatically guards against new and targeted threats by analyzing behavior before code is executed

Built-in intrusion-prevention technologies combine to detect malware, suspicious files and behavior, and deliver complete proactive protection

Norton Internet Security

Norton Internet Security works as an Antivirus protection, Internet worm protection, Personal firewall, Privacy protection, and Parental control

Features:

- Automatically detects and removes viruses, Trojan horses, and worms
- Detects and removes viruses in Internet downloads and email attachments
- Personal firewall gives you control over all incoming and outgoing Internet traffic
- Privacy control prevents information being sent without your permission
- Parental control blocks Web sites you don't want your children to visit
- Protects privacy and saves disk space by removing unwanted cookies and cache files

Norton Internet Security: Screenshot

MAC OS X Security Tools

MacScan

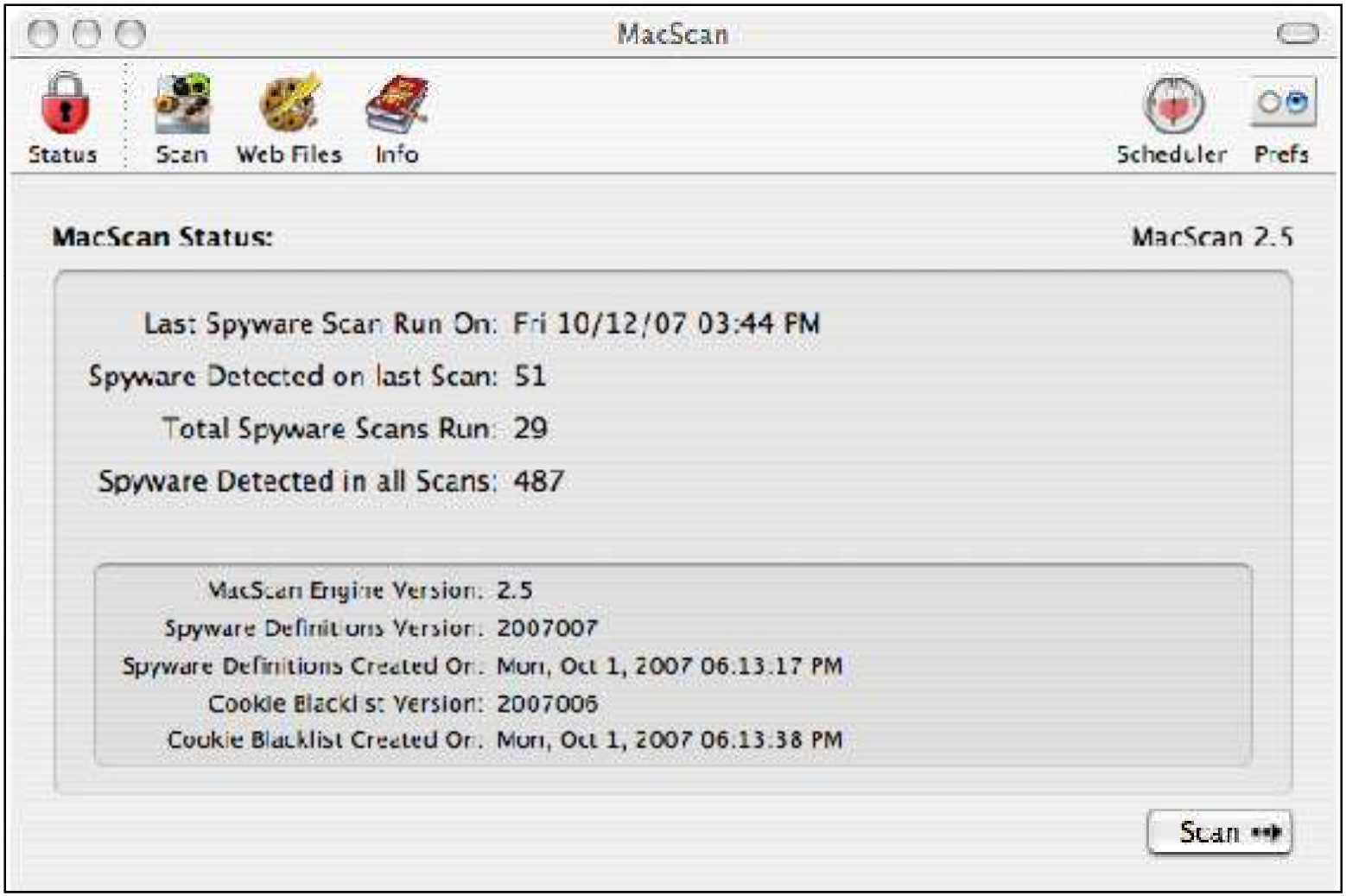
MacScan can detect, isolate, and remove the program which could allow remote administration and violate security using advanced detection methods

Many remote administration programs used by hackers to gain remote access to your computer often goes undetected as antivirus software does not commonly protect from spyware

MacScan detects, isolates, removes, and also informs if any remote administration applications are active

MacScan also audits and protects the system from spyware programs such as keystroke recorders

MacScan: Screenshot



ClamXav

ClamXav is a free virus checker for Mac OS X

ClamXav is built upon the popular free ClamAV open source command line antivirus engine and converts it into an easy to use interface

This software has the ability to move files on your computer, therefore, it is absolutely vital that you back up any important data before running ClamXav

ClamXav: Screenshot

IPNetsentryX

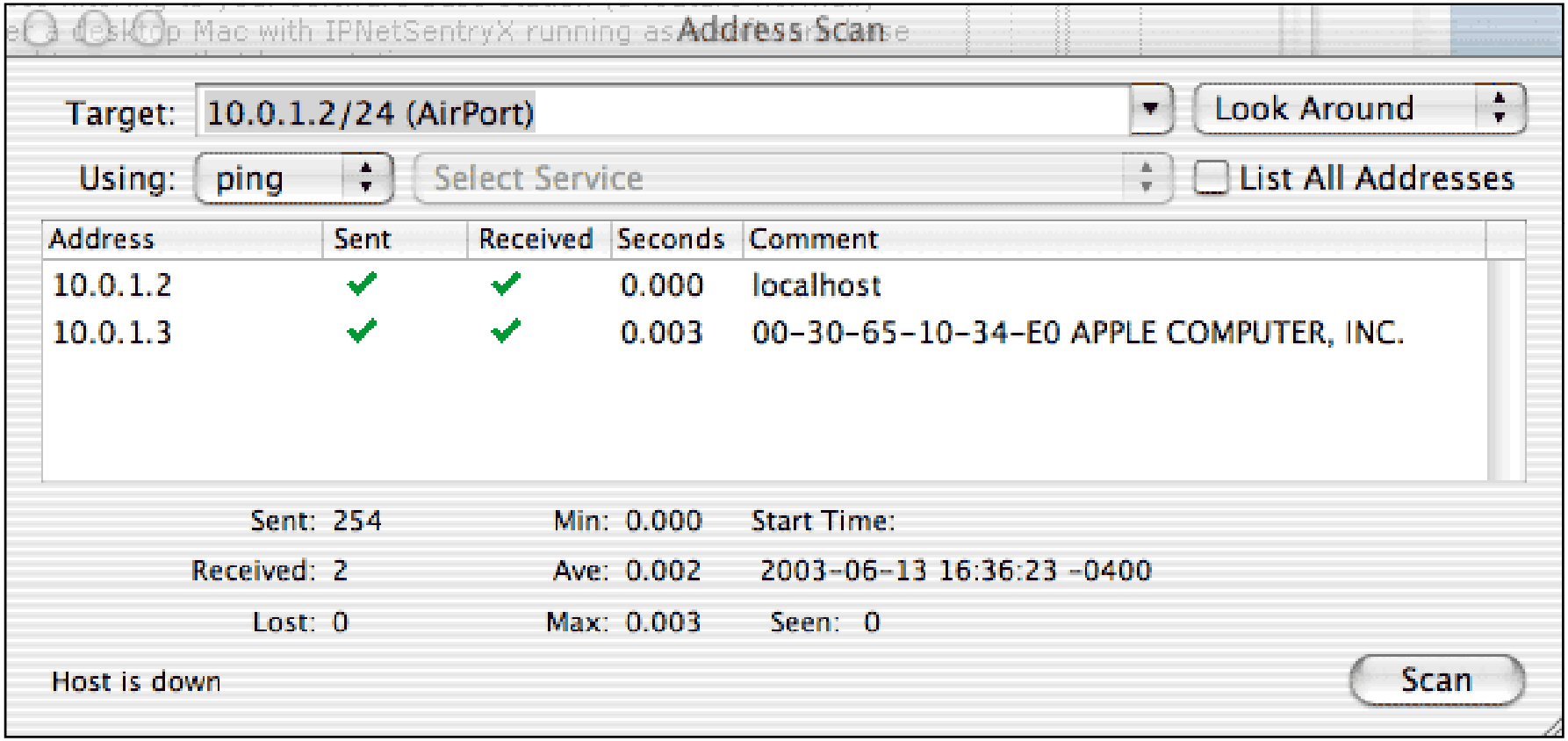
IPNetSentryX is a simple and intelligent security application which protects your Macintosh from outside intruders and other undesirable network traffic

This is particularly important for Macintosh users who have cable modem, DSL, or other high-speed Internet service

Features:

- Provides intelligent protection without expert configuration
- Hierarchical filter rules offer exceptional control over network traffic
- Supports data content filtering to stop Internet worms
- Safely ignores promiscuous TCP resets
- Show firewall rules in action
- Includes tools to identify the source of suspected intruders
- Flexible network event monitoring and Email notification

IPNetsentryX: Screenshot



FileGuard

FileGuard allows multiple users to have restrained access; this can be done by file privileges and login periods

The computers can be restricted to certain days and certain time

FileGuard as the administrator has full control over the users and the log files

Other feature of this program besides the security of locking your computer down is the file shredding ability

FileGuard: Screenshot

Countermeasures

- Turn off File sharing, guest file sharing access, access to the machine's owner via file sharing when not in use
- Turn off personal web sharing and program linking
- Check the configuration and status of third-party applications and system extensions which may provide additional network-accessible services
- Install a commercial anti-virus which acts as personal firewall and keep up to date with new versions
- Use Apple or third party tools to encrypt sensitive documents and to create password-protected, encrypted volumes on which to store documents
- Perform regular backups
- Rotate three or more backup sets, and keep at least one recent backup set off site

Summary

- Mac OS X is a uniquely powerful development platform, bringing a 32-bit and 64-bit architecture and multiprocessor capability to the desktop and server arenas
- SLP daemon (Service Location Protocol) advertises local services to the network
- Multiple binaries inside the directory tree are setuid root, but remain writable by users in the admin group, which allows privilege escalation
- Crafted HFS+ filesystem in a DMG image can cause the do_hfs_truncate() function to panic the kernel (denial of service), when trying to remove a file from the mounted filesystem

"I have no objection to creative problem solving as long as it's not too creative and it's not a real problem."