Global Information Assurance Certification Paper

Securing Mac OS X 10.1.5 Using Free Software

David A. Shinberg

Security Essentials Certification (GSEC) - Practical Assignment
Version 1.4 (amended April 8, 2002)

1. Abstract

Mac OS X is a UNIX based operating system for Apple Macintosh computers. The switch from the earlier proprietary Macintosh operating systems to Mac OS X provides several security challenges and advantages to classic Macintosh users. Before OS X, users had a very limited choice of software to enhance the security of their computer. Additionally, most of this software was commercial.

The specific host protection tools being evaluated are: Firewalls, Intrusion Detection Systems, and Virus detection and removal utilities.

This paper evaluates how to secure Mac OS X using inherent capabilities of the operating system as well as freeware tools. The free options are compared against some commercial options focusing on which choices are best for an experienced Mac user, but novice UNIX user.[1]

1. Security Concerns for the Home User

With the advent of broadband access, home users are susceptible to attacks that were previously focused on corporate and academic facilities. There are several reasons why high-speed access to home computers makes them better targets. One reason is that the computer is connected to the Internet whenever it is turned on. This means that there is a higher probability that the attacker will find a given computer compared to when the computer only accessed the Internet via a dialup connection. Another reason is that an attacker has more to gain from compromising a computer with high-speed Internet access because the compromised computer can be used to launch more attacks.

The Federal Trade Commission (FTC) recently released a two-page paper that highlights some important security items that pertain to high-speed users.[2] The items that pertain to this paper are:

---

[1] Although Mac OS 10.2 (Jaguar) was released in August 2002, the system used for this paper is using a fully patched version of Mac OS 10.1.5.

[2] Federal Trade Commission "Safe at Any Speed: How To Stay Safe Online if You Use High-Speed Internet Access. "
http://www.ftc.gov/bcp/conline/pubs/online/safeonline.htm

- Use anti-virus software
- Regularly update anti-virus software
- Install a firewall
- Take advantage of your software's security features
- Turn off software features that you don't use

The FTC paper also covers security issues related to social engineering. Although reading email from an unknown source is a bad idea, these issues are not included in this paper. The information in the FTC paper should be required reading for all novice broadband users. Although FTC paper supports areas that are evaluated in this paper, the topic of this paper was chosen and the abstract written before the FTC paper was published.

2. Methodology

The methodology used was to evaluate commercial security software and determine if free software could provide the same level of security. Another and more important aspect of the comparison is the ease of use of the various packages. While the usability of the software is not critical to an advanced users, who might be perfectly comfortable editing firewall rules, usability is extremely important to most home users.

Tests of the firewall wall were performed by scanning the test system using nmap. Nmap provided a simple interface and was capable of triggering alerts on the firewall. The virus scanners were verified using the ICAR standard test signature.

3. Available Software

Several commercial and free packages enhance the security of Mac OS 10.1.5. Additionally, a capable ipfw is built into this operating system. Commercially available and freeware packages are described in the following sections.

3.1. Commercial Software

The primary vendors supplying security software for the Mac OS X are Intego, McAfee and Norton by Symantec. All three companies provide antivirus, firewall and content filtering software. The test system used Intego NetBarrier for a firewall and Virex for virus protection.

Intego describes the NetBarrier product as follows.[3]

---

[3] Information from Intego's website http://www.intego.com/netbarrier/, obtained August 31, 2002.

NetBarrier's **Personal Firewall** protects and monitors all incoming and outgoing data. A customized mode allows you to create your own defense rules, offering the most secure level of protection.

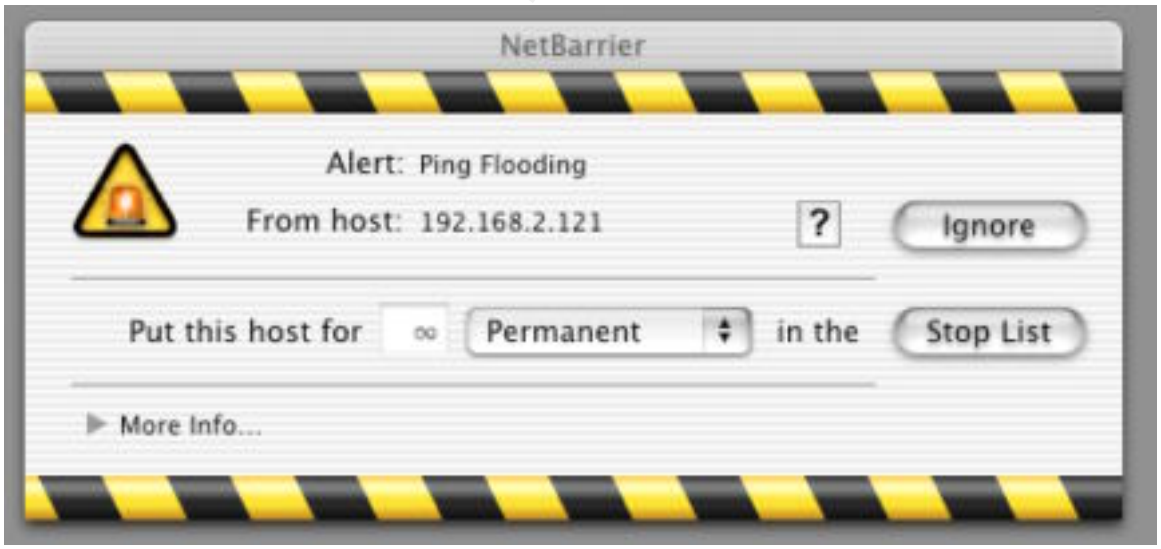
NetBarrier's **Antivandal** blocks all attempts to break into your Mac, detects wrong passwords and logs vandal attacks for complete protection. Moreover, it has an alarm to inform you of every intrusion attempt.

NetBarrier's **Internet Filter** analyzes data as it leaves your computer and prevents unauthorized exporting of private information such as credit card numbers, passwords, sensitive data and more...

NetBarrier's **Internet Privacy** feature helps maintain your privacy, giving you control over cookies, blocking ad banners and blocking spam before you even download it. NetBarrier also helps cover your tracks, by refusing to give out certain personal information.

The Firewall, Antivandal are features that are available in ipfw as described in section 4.5. The Internet filter and privacy feature are not available in ipfw. These additional protection features help protect a home user, but would not be useful on a server.

Simple testing with nmap resulted in the following alert being displayed by NetBarrier. The alert indicates that NetBarrier detected a “Ping Flood”, which is too many ping packets being sent to the host computer.



NetBarrier will display similar alerts whenever it detects prohibited behavior. An important feature of NetBarrier is a “Stop List”. The “Stop List” is list of hosts that will not be allowed to connect to the host computer. By default whenever an alert is triggered, NetBarrier provides the option of adding the offending host to the “Stop List”. Another configuration option will instruct NetBarrier to add any offending host to the “Stop List” automatically.

According to Intego, VirusBarrier provides the following features:[4]

- Simple, fast and non-intrusive
- Protects against all known viruses
- Protects against Word and Excel macro-viruses
- Functions in the background, all the time
- Drag and drop virus scans
- Scans Stuffit archives
- Automatically repairs infected files
- Creates log of infected files
- Detects corrupted files
- Turbo mode speeds up scanning
- Contextual Menu module for quick scans
- Menu for quick access to the control panel
- Choice of alerts - voice alert, alert screen or e-mail alert
- Password protection of the program
- NetUpdate provides automatic updates

The other commercial packages provided a similar set of capabilities. The purpose of this paper is not to critique the commercial packages. Therefore, the reader is referred to the vendors for more information on their products. Contact information for the vendors is shown below:

Company	Products	URL
Intego	NetBarrier, VirusBarrier, and ContentBarrier	www.intego.com
NAI	Virex	www.nai.com
Symantec	Norton Personal Firewall, Norton AntiVirus, and Norton Internet Security	www.symantec.com/sabu/nis/nis_mac/

3.2. Free Software

Several free software packages are available that enhance the security of Mac OS X. The following free software shown below was evaluated to determine its effectiveness and ease of use for novice users.

[4] Information from Intego's website http://www.intego.com/virusbarrier/home.html, obtained August 31, 2002.

Name	Purpose / Notes	URL
Snort	Command line intrusion detection system	www.snort.org
HenWen	Mac front end for Snort	dreamless.home.attbi.com/
VirusHammer	Java virus checker from the OpenAntiVirus Project	www.openantivirus.org/
Clam AntiVirus	Command line virus checker	clamav.elektrapro.com/
Ipfw	Built in firewall	

More details on the free software packages in provided in the following sections.

4. Installation

Default installations of the commercial software were used. This software was already installed on the system. The default configuration of the commercial software was also used.

Installation and configuration of the freeware was more complex for each package. Some packages required downloading and compiling source code, while other packages just needed to be downloaded from the web. The specific freeware packages tested are discussed in the following sections. Each section describes the process used to install, configure and test the software. However, it is assumed that the user can download the software from the web site and extract it from the archive if needed. Wherever possible the software was without administrator (i.e., root privileges).[5]

4.1. VirusHammer

VirusHammer provided by the Open AntiVirus Project is a Java application that performs virus scanning of files. VirusHammer requires Java WebStart that is included in Mac OS X. Downloading and running VirusHammer was trivial and VirusHammer correctly identified the test files that contained the EICAR test signature.[6]

VirusHammer has an extremely easy to use graphical user interface. The user can add the files and or directories to be scanned to using the add button. The results of the scan are shown in the bottom portion of the window.

---

[5] Even though it is based on Unix, Mac OS X does not permit users to log into the root account. When root or administrator privileges are needed, a dialog box appears requesting the administrator password. The other method to gain root privileges is to use sudo.

[6] OpenAntiVirus Website http://www.openantivirus.org

4.2. Clamscan

Clamscan is an open source command line virus scanner written in C. Clamscan was obtained from http://clamav.elektrapro.com/ and compiled without any complications using the following commands:

```
$ ./configure --disable-clamav > configure.log 2>&1
```

Mac OS X does not have the useradd or groupadd commands, so it was necessary to use the –disable-clamav option to disable the need for the clamav account and group.

Clamscan was able to identify the test files that contained the EICAR test signature. It is possible to configure Clamscan to run via a cron job. Additionally, freshclam can be used to automatically update the virus signatures from the OpenAntiVirus site.

The following is an example of running clamscan in the directory that contains the virus test files.

```
$ pwd
/Users/das/Security/Virus Test Files
$ clamscan
/Users/das/Security/Virus Test Files/eicar.com: Eicar-Test-Signature
FOUND
/Users/das/Security/Virus Test Files/eicar.com.txt: Eicar-Test-
Signature FOUND
/Users/das/Security/Virus Test Files/eicar_com.zip: Eicar-Test-
Signature FOUND
/Users/das/Security/Virus Test Files/eicar_resource_fork: Empty file.
/Users/das/Security/Virus Test Files/eicarcom2.zip: Eicar-Test-
Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 1786
Scanned directories: 1
Scanned files: 5
Infected files: 4
Data scanned: 0.00 Mb
I/O buffer size: 131072 bytes
Time: 0.461 sec (0 m 0 s)
$
```

The freshclam command allows the user to quickly and simply updated the virus signatures used by clamscan. An example of updating the virus signatures is shown below.

```
$ freshclam
Checking for new database - started at Thu Sep 19 21:39:50 2002
Connected to clamav.elektrapro.com.
Reading md5 sum of database from clamav.elektrapro.com : OK
```

```
Downloading database from clamav.elektrapro.com
.....................................................................
.....................................................................
.....................................................................
.................................................... done
Database updated.
$
```

4.3. SNORT

The latest version of snort was obtained from www.snort.org. SNORT requires libpcap, which is installed on Mac OS X. Therefore it should have been simple to run the following command to compile the snort.

```
$ ./configure > configure.log 2>&1
$ make > make.log 2>&1
```

However, the make failed because it could not find libpcap.h. Searching the system using find, revealed that libpcap.h did not exist! Therefore, it was necessary to download and install libpcap from www.tcpdump.org.

```
/Users/das/Security/libpcap-2002.08.22
$ ./configure > configure.log 2>&1
```

Libpcap is aware of Mac OS X as indicated by the following entries in configure.log.

```
checking host system type... powerpc-apple-darwin5.5
checking target system type... powerpc-apple-darwin5.5
checking build system type... powerpc-apple-darwin5.5
```

Compiling libpcap, as shown below, was successful and libpcap was installed into its default location which is /usr/local.

```
$ make > make.log 2>&1
```

With libpcap installed in /usr/local, SNORT needed to configured to find libpcap and then compiled

```
/Users/das/Security/snort-1.8.7
$ ./configure --with-libpcap-includes=/usr/local/include --with-
libpcap-libraries=/usr/local/lib > configure.log 2>&1

$ make > make.log 2>&1
```

Snort was tested in sniffer mode and functioned normally. Configuring Snort was also straightforward. Several snort rules are provided in the distribution. Snort was able to detect nmap scans of the test machine and log the information appropriately.

4.4. HenWen and LetterStick

HenWen and LetterStick are freeware programs written by Nick Zitzmann. All that is required to install HenWen and LetterStick is to down load the appropriate file, and drag the contents of the diskimage to a local folder on the computer. HenWen provides an easy to use front end to Snort and is distributed with a version of Snort compiled for Mac OS X. HenWen eliminates the need for the user to understand the Snort rules and choose an appropriate set of rules. The configuration of Snort is performed through a simple graphical user interface. HenWen also allows the user to add custom Snort rules if desired.

LetterStick provides the ability to produce dialog boxes whenever a Snort Alert is triggered. This is important because most novice users, and several advanced users will not bother to check the systems logs on a regular and frequent basis. The dialog box shown below was generated by LetterStick when Snort detected a ping scan.

HenWen is free for home and non-profit use; however, it has a shareware fee of $25.00 for commercial users.

4.5. IPFW

IPFW is a packet filtering firewall that is built into Mac OS 10.1.5. It is similar if not the same firewall as the ones derived from FreeBSD. IPFW is configured using the ipfw command. The script used to configure IPFW is shown below.[7]

---

[7] The articles by Dru Lavigne were used as a guide in producing the ipfw configuration.

```
# Some simple firewall rules for a host
# This comes from:
# http://www.onlamp.com/pub/a/bsd/2001/05/09/FreeBSD_Basics.html
ipfw flush
ipfw add 00100 allow ip from any to any via lo0
ipfw add 00200 deny ip from any to 127.0.0.0/8
#ipfw add 00300 check-state
ipfw add 00302 allow tcp from any to any out setup
ipfw add 00351 allow tcp from any to any in established
ipfw add 00352 deny log tcp from any to any in tcpflags syn

# The following line handles DNS queries
ipfw add 00400 allow udp from 192.168.2.1 to any in recv en0
ipfw add 00403 allow udp from any to any out
#The following line handles DHCP from my home firewall.
ipfw add 00501 allow udp from 192.168.2.1 67 to any 68 in recv en0
# The following rules allow ICMP messages
# Destination Unreachable
ipfw add 00600 allow icmp from any to any icmptype 3
# Source quench
ipfw add 00601 allow icmp from any to any icmptype 4
# Echo Request Can be sent
ipfw add 00602 allow icmp from any to any out icmptype 8
# Echo Reply can be recieved but not sent!
ipfw add 00603 allow icmp from any to any in icmptype 0
# Time Exceeded
ipfw add 00604 allow icmp from any to any in icmptype 11
#ipfw add 6500 deny ip from any to any
```

A sample application of the above rules follows:

```
[localhost:~/Security] root# /bin/sh ipfw.conf
Are you sure? [yn] y

Flushed all rules.
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00302 allow tcp from any to any out setup
00351 allow tcp from any to any in established
00352 deny log tcp from any to any in tcpflg syn
00400 allow udp from 192.168.2.1 to any in recv en0
00403 allow udp from any to any out
00501 allow udp from 192.168.2.1 67 to any 68 in recv en0
00600 allow icmp from any to any icmptype 3
00601 allow icmp from any to any icmptype 4
00602 allow icmp from any to any out icmptype 8
00603 allow icmp from any to any in icmptype 0
00604 allow icmp from any to any in icmptype 11
```

The functioning of the rules was checked by browsing the web and recording examining the firewall table as shown below.

```
[localhost:~/Security] root# ipfw -a list
```

```
00100 548  62312 allow ip from any to any via lo0
00200   0      0 deny ip from any to 127.0.0.0/8
00302  20   1200 allow tcp from any to any out setup
00351 135  91718 allow tcp from any to any in established
00352   0      0 deny log tcp from any to any in tcpflg syn
00400  18   3876 allow udp from 192.168.2.1 to any in recv en0
00403  18   1123 allow udp from any to any out
00501   0      0 allow udp from 192.168.2.1 67 to any 68 in recv en0
00600   0      0 allow icmp from any to any icmptype 3
00601   0      0 allow icmp from any to any icmptype 4
00602   0      0 allow icmp from any to any out icmptype 8
00603   0      0 allow icmp from any to any in icmptype 0
00604   0      0 allow icmp from any to any in icmptype 11
65535 988 114703 allow ip from any to any
```

The rule numbered 65535 is the default accepts all rule under Mac OS X. It is surprising that Apple chose to accept all packets as the default as opposed to denying them.

5. Evaluation and Recommendations

The evaluation of the virus protection software was performed using the EICAR standard virus signature test. All software detected the signature in the two regular and two archive files that contained the signature.

The freeware virus scanners are effective at finding viruses in files in Mac OS X. There is a potential problem with these tools in earlier version of Mac OS. The problem is prior to Mac OS X; files on a Mac were composed of two parts. One part is the data fork that stores what is normally thought of as the file content. The other part is the resource fork that stores the resources associated with a file. Resources include icons and configuration information. Prior to the advent of the Power PC based Macs; the resource fork also contained executable code.

The freeware virus scanners are incapable of scanning the resource forks of Macintosh files. This means that it is possible for some infections to be missed. Additionally, the freeware scanners do not provide the ability to clean infected automatically, nor do they provide on access scanning and notification.

The evaluation of the intrusion detection systems and firewalls was performed by evaluating the responses to nmap scans. Both a TCP and UDP scans were performed from a machine running RedHat Linux 7.1. Both the ipfw firewall and NetBarrier, when properly configured, blocked access to the test computer. An interesting result was that nmap reported the ports as filtered.

5.1. Detailed Firewall and IDS testing

This section provides in-depth technical discussion on the procedures used to test the Firewall and IDS tools being evaluated. Less technical readers may want to skip this section and proceed directly to section 6, Conclusion, on page 15.

To facilitate the testing of the firewalls and intrusion detection systems scripts were used on the Linux box.

The first test was to establish a baseline for the test machine. The test machine was configured to allow ssh and ftp access and both ipfw and NetBarrier were disabled. By default, Mac OS X is configured with all remote access disabled. [8] The baseline script is shown below.

```
# Note: Test performed with ftp and ssh enables
# router was disconnected from the cable modem
# Netbarrier configured to no protection
# only OS default ipfw rule which is allow all.

# Services Scan
nmap -n -r -sS -sU -v -oN baseline.port.out 192.168.2.42 >>
nmap.baseline.trace 2>&1

# Stack and OS identification
nmap -n -r -sO -O -v -oN baseline.os.out 192.168.2.42 >>
nmap.baseline.trace 2>&1
```

The file baseline.port.out contained the following information.

```
# nmap (V. 2.54BETA30) scan initiated Wed Sep 18 19:43:10 2002 as: nmap
-n -r -sS -sU -v -oN baseline.port.out 192.168.2.42
Interesting ports on  (192.168.2.42):
(The 2995 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
68/udp     open        bootpc
123/udp    open        ntp
514/udp    open        syslog
846/udp    open        unknown


# Nmap run completed at Wed Sep 18 19:43:36 2002 -- 1 IP address (1
host up) scanned in 26 seconds
```

Notice that the only to open TCP ports are for ftp and ssh, which is as expected. However, there are several UDP ports open! The bootpc port (68) allows the test machine to use DHCP to obtain its IP network information. The ntp port (123) is for the network time protocol used to set the clock automatically. The syslog port (514) is for the Unix syslog system. However, UDP port 846 is listed as unknown.

[8] During the baseline test, the router connected to the cable modem was disconnected from the cable modem to ensure that the test machine was not attacked during the baseline test.

This was originally troublesome; however, after a little research this port is used by Apple for its NetInfo service.[9]

Another feature of nmap is its ability to perform Operating System Fingerprinting. The results of attempted protocol and operating system identification are shown below.

```
# nmap (V. 2.54BETA30) scan initiated Wed Sep 18 19:43:36 2002 as: nmap
-n -r -sO -O -v -oN baseline.os.out 192.168.2.42
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting protocols on  (192.168.2.42):
Protocol   State       Name
1          open        icmp
…           …           …
254        open        unknown

Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i686-pc-linux-gnu%D=9/18%Time=3D890FBC%O=-1%C=-1)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DA
T=E)

# Nmap run completed at Wed Sep 18 19:43:56 2002 -- 1 IP address (1
host up) scanned in 20 seconds
```

All of the protocols report to be open. This is highly unlikely and probably due to a bug in nmap. More interestingly, nmap was not able to identify the operating system. At the least, one would have expected nmap to determine that Mac OS X is based on BSD. In addition, Darwin, which is the open source component of Mac OS X, has been available for years.

The next test configuration enabled NetBarrier and set it to client only. The client only mode allows all connections originated from the test machine to be established. Additionally, NetBarrier provides protection against port scans.

The following script was used to test NetBarrier. Please not that the –P0 option is required because NetBarrier prevented the test machine from respond to ping requests.

```
# Note: Test performed with ftp and ssh enables
# router was disconnected from the cable modem
# Netbarrier configured to no client only and other defaults
```

---

[9] AppleCare Knowledgebase Document “"Well Known" TCP and UDP Ports Used By Apple Software Products”

```
# only OS default ipfw rule which is allow all.

# Need to turn on -P0 because ping requests are not being returned
# Services Scan
nmap -n -r -sS -sU -P0 -v -d -oN netbarrier-2.port.out 192.168.2.42 >
nmap.netbarrier-2.trace 2>&2

# Stack and OS identification
nmap -n -r -sO -O -P0 -v -d -oN netbarrier-2.os.out 192.168.2.42 >>
nmap.netbarrier-2.trace 2>&2
```

Excerpts from the results of the port scan to evaluate NetBarrier are shown below.

```
# nmap (V. 2.54BETA30) scan initiated Wed Sep 18 21:15:46 2002 as: nmap
-n -r -sS -sU -P0 -v -d -oN netbarrier-2.port.out 192.168.2.42
Interesting ports on  (192.168.2.42):
(The 1549 ports scanned but not shown below are in state: filtered)
Port       State       Service
1/udp      closed      tcpmux
…           …           …
68/udp     open        bootpc
69/udp     closed      tftp
…           …           …
123/udp    open        ntp
124/udp    closed      ansatrader
…           …           …
846/udp    open        unknown
847/udp    closed      unknown
…           …           …
54321/udp  closed      bo2k

# Nmap run completed at Wed Sep 18 21:44:12 2002 -- 1 IP address (1
host up) scanned in 1706 seconds
```

NetBarrier is effective in protecting the test machine as indicated that all TCP ports are filtered. Again, a select number of UDP ports are open. However, by examining the results a hacker can determine that the test machine is running a firewall. The reason is that the TCP ports are filtered as opposed to closed.

The final firewall test was performed with ipfw configured as described in section 4.5, and NetBarrier disabled. The script used to test the ipfw configuration is shown below.

```
# Note: Test performed with ftp and ssh enables
# router was disconnected from the cable modem
# Netbarrier disabled.
# ipfw was enabled.

# Need to turn on -P0 because ping requests are not being returned
# Services Scan
nmap -n -r -sS -sU -P0 -v -oN ipfw-1.port.out 192.168.2.42 > nmap.ipfw-
1.trace 2>&2

# Stack and OS identification
```

```
nmap -n -r -sO -O -P0 -v -oN ipfw-1.os.out 192.168.2.42 >> nmap.ipfw-
1.trace 2>&2
```

Excerpts from the results of the port scan to evaluate ipfw are shown below.

```
# nmap (V. 2.54BETA30) scan initiated Thu Sep 19 06:04:14 2002 as: nmap
-n -r -sS -sU -P0 -v -oN ipfw-1.port.out 192.168.2.42
Interesting ports on  (192.168.2.42):
(The 1549 ports scanned but not shown below are in state: filtered)
Port       State       Service
1/udp      closed      tcpmux
…           …           …
68/udp     open        bootpc
69/udp     closed      tftp
…           …           …
123/udp    open        ntp
124/udp    closed      ansatrader
…           …           …
846/udp    open        unknown
847/udp    closed      unknown
…           …           …
54321/udp  closed      bo2k

# Nmap run completed at Thu Sep 19 06:32:20 2002 -- 1 IP address (1
host up) scanned in 1686 seconds
```

The results show that both NetBarrier and ipfw have the same nmap signature. The built-in ipfw firewall can effectively protect a system providing the correct rules are used. The problem with ipfw in Mac OS 10.1.5 is that it is too difficult for a novice user to configure.[10] Additionally, the freeware products do not include the capability to display dialog boxes when an alert is triggered.

The evaluation of the IDSs was done by examining the packets that they detected. The performance of NetBarrier was discussed in section 3.1. The problem with snort is that the logs are difficult to read. For example, here is an excerpt fro the portscan.log file.

```
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:998 SYN ******S*
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:999 SYN ******S*
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:1000 SYN ******S*
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:1001 SYN ******S*
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:1002 SYN ******S*
Sep 19 06:13:50 192.168.2.121:57289 -> 192.168.2.42:1003 SYN ******S*
Sep 19 06:13:56 192.168.2.121:57289 -> 192.168.2.42:1004 SYN ******S*
```

[10] The author has heard that Mac OS 10.2, also known as jaguar, will have an easy method for configuring ipfw; however, this information could not be confirmed from Apple's web site.

The log shows that a port scan is taking place. However, a novice user would have trouble finding the log in /var/log/snort and more importantly understanding its contents.

Snort provides even more detail, as shown below

```
$ more TCP:57289*
::::::::::::::
TCP:57289-1080
::::::::::::::
[**] SCAN SOCKS Proxy attempt [**]
09/19-06:14:08.949289 192.168.2.121:57289 -> 192.168.2.42:1080
TCP TTL:40 TOS:0x0 ID:25191 IpLen:20 DgmLen:40
******S* Seq: 0x760E934E  Ack: 0x0  Win: 0x400  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
+=+

::::::::::::::
TCP:57289-3128
::::::::::::::
[**] SCAN Squid Proxy attempt [**]
09/19-06:16:21.404612 192.168.2.121:57289 -> 192.168.2.42:3128
TCP TTL:40 TOS:0x0 ID:35894 IpLen:20 DgmLen:40
******S* Seq: 0x760E934E  Ack: 0x0  Win: 0x400  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
+=+

::::::::::::::
TCP:57289-8080
::::::::::::::
[**] SCAN Proxy (8080) attempt [**]
09/19-06:17:09.569830 192.168.2.121:57289 -> 192.168.2.42:8080
TCP TTL:40 TOS:0x0 ID:9504 IpLen:20 DgmLen:40
******S* Seq: 0x760E934E  Ack: 0x0  Win: 0x400  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
+=+
```

This is useful information because it provides more details than are in the portscan.log file. Yet, this is incomprehensible to novice users, and probably most experienced Mac users who do not have a strong UNIX or networking background.

6. Conclusion

There are both commercial and free software that can be used to increase the security of Mac OS X. An experienced Unix user or preferable an administrator can use the tools to secure a machine. However, there will still be the need to monitor the logs generated by the freeware tools.

The freeware virus tools do not provide two important features that exist in the commercial tools. The first feature is on access virus detection, which is detected a virus when a file is accessed by an application. The freeware tools do not provide this feature because the operating system must be modified to support

on access virus detection. The second feature is detecting a virus as it is transmitted over the network, commonly through email.

While snort does a better job as an IDS than the commercial tools, it does not automatically block offending hosts. NetBarrier can also scan the content of packets to ensure that personal information does not leave the computer. Well, actually this is what NetBarrier claims. It has no way of scanning and thus stopping encrypting information.

There is a popular feature of ZoneAlarm, which is a popular Windows firewall that is absent from the Mac. ZoneAlarm, will only allow authorized applications to access the network. There are two types of authorized access that this prevents. The first is legitimate applications that use the network to enforce license terms, or send usage data to a remote host. The second and in most cases more serious are Trojan horses that open ports. A Mac user can use the netstat command to list the open ports; however, this is cumbersome and only lets the user know something is wrong after the fact.[11]

The commercial tools are better suited for a novice user as they are easy to use and provide better feedback about security issues. A novice user or even an experienced user, who does not want to worry about examining logs, will be better served by purchasing the appropriate commercial tools.

[11] NetBarrier can be configured to limit the outbound connections that can be established based on port number. An example of this more secure configuration is provided in Appendix A.

References

Federal Trade Commission "Safe at Any Speed: How To Stay Safe Online if You Use High-Speed Internet Access. " http://www.ftc.gov/bcp/conline/pubs/online/safeonline.htm

Apple Computer, Inc. "I n s i d e M a c O S X: System Overview © 2000–2002 Apple Computer, Inc. , July 2002. http://developer.apple.com/techpubs/macosx/Essentials/SystemOverview/SystemOverview.pdf

European Institute for Computer Anti-Virus Research, http://www.eicar.org/, last accessed 2 September 2002

OpenAntiVirus Project Website, http://www.openantivirus.org/, last accessed 2 September 2002

Clam AntiVirus Website, http://clamav.elektrapro.com/, last accessed 2 September 2002

Palmer, Gary and Nash, Alex FreeBSD Handbook Chapter 10 Section 7 "Firewalls", http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html, last visited 2 September 2002

Zitzmann, Nick "Hen Wen User's Manual for Version 1.1", © 2002. (Part of HenWen Distribution)

Mac OS X Security Introduction, http://developer.apple.com/internet/macosx/securityintro.html, last visited 2 September 2002

Lavigne, Dru, "BSD Firewalls: IPFW". http://www.oreillynet.com/pub/a/bsd/2001/04/25/FreeBSD_Basics.html, last visited 28 August 2002.

Lavigne, Dru, "BSD Firewalls: IPFW Rulesets", http://www.oreillynet.com/pub/a/bsd/2001/05/09/FreeBSD_Basics.html, last visited 28 August 2002.

Lavigne, Dru, "BSD Firewalls: Fine-Tuning Rulesets". http://www.oreillynet.com/pub/a/bsd/2001/06/01/FreeBSD_Basics.html, last visited 28 August 2002.

nmap website http://www.insecure.org/nmap/, last visited 2 September 2002.

AppleCare Knowledgebase Document “"Well Known" TCP and UDP Ports Used By Apple Software Products” Article ID: 106439; http://docs.info.apple.com/article.html?artnum=106439, last visited 18 September 2002.

NetBarrier X User’s Manual, Intego Inc. 1999-2001.

Appendix A: Improved NetBarrier Configuration

NetBarrier allows the user to specify exactly what traffic will be allowed in and out of the computer. The screen shot below shows a configuration that provides more security than the “Client Only” Choice.

The specific services are listed, and NetBarrier automatically adds the corresponding inbound connections. This is similar to the way ipfw handles established connections.

Last Updated: September 23rd, 2017

Upcoming Training

SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive