2006

Personal Firewalls - Testing Robustness

Patryk Szewczyk
Edith Cowan University

Craig Valli
Edith Cowan University

Personal Firewalls – Testing Robustness

Patryk Szewczyk
Craig Valli

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au

Abstract

Consumers require personal firewalls that are highly secure, easy to use, configurable and up-to-date with the latest signatures to detect malicious network activity. Robustness tests were performed on a selection of the ten most popular firewalls by market share. The test system used was a vanilla installation of Windows XP with SP2 and all the most recent updates and patches. Each firewall was installed with its default configuration following the didactic instructions given by the firewall. The investigation was carried out by performing an installation, penetration, performance and update test. A third party bitTorrent application was also installed mimicking a home installation of a download application. The Comodo Personal Firewall out performed all the firewalls which were tested including the highly popular ISS Blackice and Zonelabs ZoneAlarm. The results identified that a third party application has a significant impact on the number of vulnerabilities present within the test system.

Keywords

Firewall testing, nessus, p0f, nmap

INTRODUCTION

The past ten years has seen the emergence of people of all ages and genders utilising the Internet for their day-to-day online banking, shopping and communication requirements (Boeckeler 2004). As broadband is becoming the prevalent communication method, this is opening a whole new era of Internet experiences for home users (Droppleman 2004). What was once limited by bandwidth now permits high resolution graphics, live video steaming and flash animations. However, these benefits are at the cost of large bandwidth which may be exploited and abused by unauthorised individuals.

The availability and little modest knowledge required to use tools to carry out remote attacks and comprise client computers is constantly rising (Seshardi et al. 2006). One of the largest threats currently to computers connected to the Internet is the malicious effect of spyware. Spyware is malicious code or data which resides on a client's computer, monitoring and collecting various behavioural computer use data (Warkentin et al. 2005). Sophisticated spyware may collect user data and retransmit this information to a third party. It may also be used to initiate various marketing pop-ups and unwanted advertising, dependant on the end-users Internet usage patterns. Malicious spyware may alter the start-up page in web browsers without authorisation and acknowledgement from the end-user. This malicious activity operating on a client's computer may drastically reduce Internet connectivity speeds and lower computer performance by unknowingly operating hidden in the background.

In order to prevent malicious activity from occurring, a firewall may be utilised to stop and filter various packets from being sent or received. Firewalls are available in two distinct types, although operate in a similar manner. Network hardware including switches and routers filter packets to various destinations on a network, dependant on pre-defined sets of rules. Software firewalls follow a similar principle and are a base means of filtering network data packets through a network (Ciampa 2005). Software firewalls also known as personal firewalls use a pre-defined set of rules created by the developers. New up-to-date rules are created and added with each

further version release. Personal firewalls are a learning applications in which the end-user is required to teach the software what processes and software may operate and/or access the outside network (West 2006). In most instances users are presented with the process or application which is trying to access a particular network through a specific port. They are then presented with the choice of allowing, denying or creating a set of rules on which the firewall will operate on for future unusual occurrences. While the firewall is in operation all malicious instances of activity are generally reported and monitored through the intrusion detection system.

The intrusion detection system (IDS) monitors' network behaviour based on either an anomaly or misuse detection rule set (Fan et al. 2004). Anomaly detection identifies any traffic as malicious if it is not considered normal, and hence deters from expected or previous learned system behaviour. Alternatively misuse detection uses a signature based system which matches traffic patterns with known malicious traffic which may cause harm. In ideal well designed personal firewalls, the application should actively monitor network traffic and identify, block and inform the end-user of any unusual or malicious activity.

A personal firewall to operate effectively relies upon up-to-date databases and signatures with detailed rule sets for known malicious activity. However, it is also up to the end-user to be consciously aware and pro-active in identifying malicious versus legitimate network traffic. A personal firewall coupled with an inexperienced user may lead to little or no computer security. Software firewalls are only as good as they are implemented and configured. In some instances individuals choose to uninstall the application, rather than lowering the security settings, as default installations initially require the user to allow or deny applications and processes to network access (Frisk & Drocic 2004). Hence, it is vital that personal firewalls be robust, yet still maintains a high level of assistance and information to the in-experienced end-user to ensure that the firewall is utilised to its full potential. Previous research undertaken by Yee (2002) examined the strength of security in home use personal firewalls. The research was conducted by penetration test using default installations of personal firewalls on a base Microsoft Windows 98 system. This research follows on and builds upon the previous firewall research.

METHOD

The tests system comprised of two PC clone systems with the specifications listed in Table 1. Computer System 1 had a default installation of Windows XP Professional with Service Pack 2 with patches applied up to and including September 24th 2006. This system was the baseline image for the installation of each of the individual packages for testing. Computer System 2 was using secureDVD with the auditor boot selected.

Table 1 Specification of test systems

Computer System 1 (defender)	Computer System 2 (attacker)
Intel P4 1.4 GHz	Intel P4 1.8 GHz
Intel Motherboard	Asus Motherboard
512mb RAM	1024mb RAM
40 GB HDD	80 GB HDD

The top ten firewalls were downloaded from the Internet according to market share and popularity and are detailed in Table 2 (Markus 2006; PCWORLD 2005). Each firewall was either a limited 15/30-day trial or a free for personal use version. However, in two instances the commercial firewall was not available as a trial or free use version and required that a full version product be purchased instead. Hence, those were omitted from the study and another personal firewall situated in its place.

Each firewall was installed independently on a partition which was wiped using Helix v1.7. A clean image of Windows XP Professional with SP2 and the latest updates and patches, was produced onto the test hard disk using Norton Ghost. A set of criteria outlined further was then used against each of the personal firewalls tested.

Installation Testing

The installation test was achieved by a default installation using the supplied media and instructions. The machine was connected live to a network connection so that it would mimic a home user using ADSL. Installation in each case was only achieved by the didactic following of the instructions provided to the end user. If registration was a goal of the process this likewise was instantiated by following instructions didactically, and looked at reasons for this requirement. Points were made to determine if the end-user is informed of any changes to operating system configuration such as disabling of the Windows firewall.

Table 2 Personal firewalls tested

Product	Version
Agnitiun Outpost Firewall	1.0
Armor2net	3.12
Blackice	3.6
Comodo Personal Firewall	2.3.5.62
Keiro WinRoute Firewall	6.2.2
Norton Personal Firewall 2006	-
Panda Antivirus + Firewall 2007	6.00.00
Sunbelt Keiro Personal Firewall	4.3.268
Tiny Personal Firewall 2005	6.5.126
Zonelabs ZoneAlarm Free	6.5.737.000

Penetration Testing

This involved testing the baseline system and each subsequent firewall system with a series of known and published exploits that a competent firewall should be able to stop. A brute force scan of the system was undertaken with Nessus 3.0.3 vulnerability scanner. Nessus had been updated with the most recent plug-ins, and configured to test the system extensively by including the dangerous vulnerability plug-ins. All tests were carried out using default settings. Further to these tests system reconnaissance activities provided by nmap and p0f were undertaken. This reconnaissance involved using default modes of each program, using a scanning attack as well as ‘quiet’ and ‘sneaky’ modes intended to avoid detection.

Having completed all three of the tests to establish baseline security of the firewalls, further tests were applied while a commonly used file sharing program was in operation. The third party package applied was the original bitTorrent 4.20.7 program. Didactic following of instructions was again undertaken to enable functionality of these programs. In most instances this requires defining permissions by opening specific ports on the firewall applications.

Evaluation of Performance

The performance of each firewall was evaluated on the following three conditions.

1. Ability to detect attack by alerting and logging of the malicious attack.
2. Ability to respond to attack by either blocking or halting the attack fully.
3. Ability to record the attack within a log file, which may then be easily extracted into a format which can be readily analysed.

Ability to update

This looked at the ability to upgrade the default installation of the firewall via updates or patching. This was again undertaken via didactic adherence to the manual or instructions provided by the program. Simplicity was also a factor in terms of does an update download and install in the background, or is the end-user faced with downloading and re-installing a clean copy of the software.

RESULTS

Installation Test

Having completed an independent case study of each of the ten firewalls, it was soon evident which personal firewall was prevalent by the tests carried out. Presented in Table 3 are the results of the initial installation test. Only two applications recommended and required online registration. The application makes a specific note of this to the end-user, so that they are kept up-to-date with important product updates and information. On a vanilla installation of Windows XP Home and Windows XP Pro the firewall is enabled by default. During the install test, two of the personal firewalls mentioned and informed the end-user that it is recommended that the Windows firewall be disabled automatically during the install as this may conflict with the third party application. The remaining firewalls disabled the Windows firewall without notifying the end-user of this process.

Table 3 Installation test of each personal firewall

Product	Registration required?	Windows Firewall Disabled?
Agnitiun Outpost Firewall	✘	✘
Armor2net	✘	✘
Blackice	✘	✘
Comodo Personal Firewall	✘	✓
Keiro WinRoute Firewall	✘	✓
Norton Personal Firewall 2006	✘	✓
Panda Antivirus + Firewall 2007	✓	✓
Sunbelt Keiro Personal Firewall	✘	✓
Tiny Personal Firewall 2005	✘	✓
Zonelabs ZoneAlarm Free	✓	✓

Penetration Test

On successful completion of each scan by Nessus a tabulated results page was produced detailing a series of holes, warnings, notes and open ports which had been discovered by the brute force scanning utility (Table 4). As demonstrated by Figure 1 only the Comodo Personal Firewall and Sunbelt Keiro Personal Firewall did not leave the system exposed to any exploits.

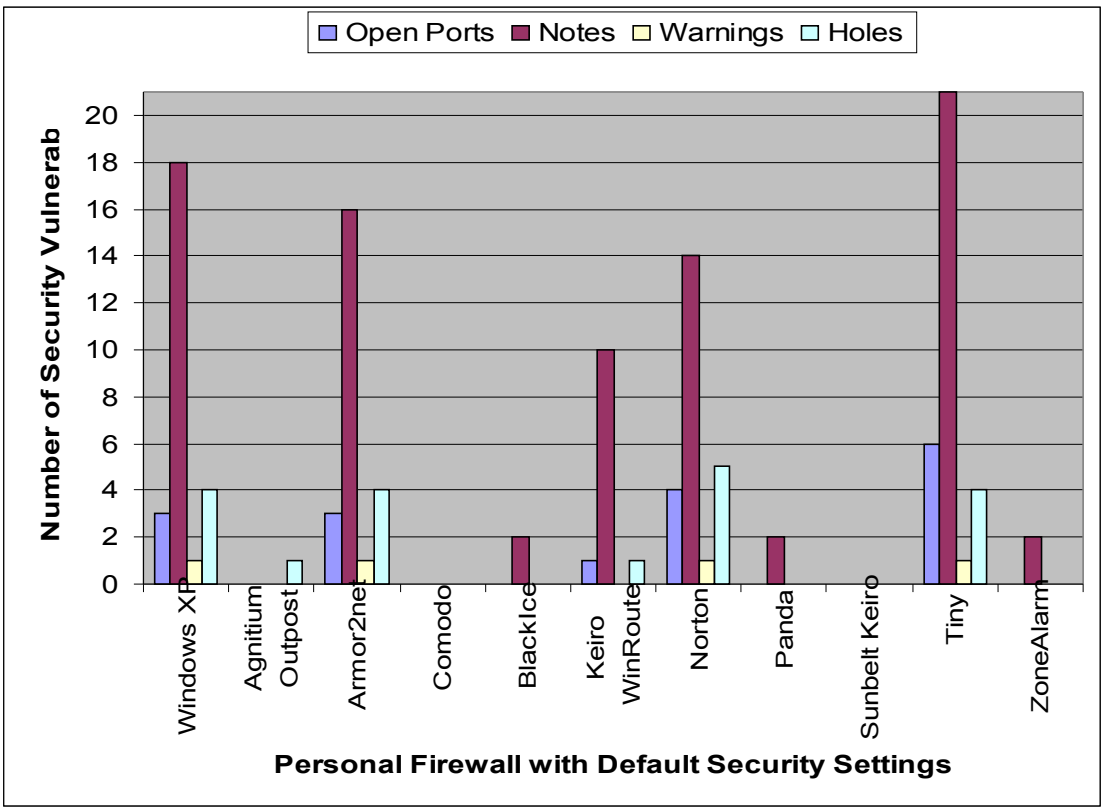

Figure 1 Nessus scan results for each firewall tested

Figure 2 shows the number of various vulnerabilities detected by Nessus when the third party original bitTorrent utility was in operation. Most of the firewalls had opened an extra port and the firewall Keiro WinRoute and Norton produced a vulnerable hole, warnings and notes depicting the extended vulnerabilities within the system when the bitTorrent utility is downloading.

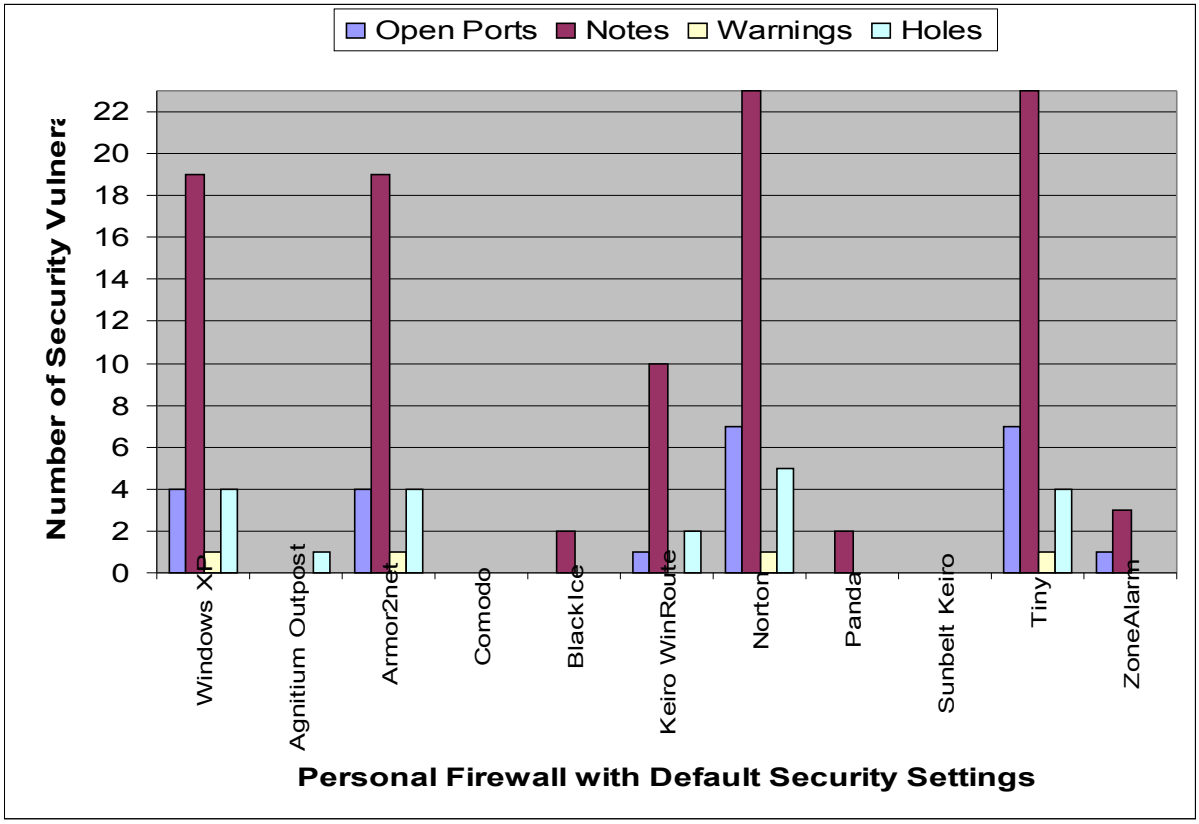

Figure 2 Nessus scan results for each firewall tested whilst using a file sharing program

Further penetration tests were executed using the passive operating system fingerprinting tool p0f. With each consecutive test of the firewall software, the correct operating system was identified by the p0f utility. The nmap test revealed slightly different results to that of Nessus with only four of the firewalls leaving ports open in contrast to Nessus which detected five firewalls with open ports. Once the third party utility bitTorrent was in operation the only extra firewall to have open ports was ZoneAlarm which is what Nessus had detected also.

Firewall Performance

Using the conditions detailed in the methodology, the performance of each firewall was analysed (Table 5). The three conditions that were examined included the ability to detect, respond and log the attacks by p0f, nmap and Nessus. No firewalls detected, responded or logged any of the malicious passive activity by p0f and hence have not been included within the performance results. Of the ten personal firewalls, five had detected and alerted the end-user of each of the attacks carried out by Nessus and nmap. Tiny Personal Firewall 2005 was the only personal firewall which was not able to meet the criteria of both detecting and alerting the end-user of the attack. The attacks were blocked fully by only two of the ten firewalls, Comodo Personal and Sunbelt Keiro Personal. This is comparatively lower than the number of firewalls which had only detected the attack. The evidence suggests that although the attacks were detected by the firewalls, they were not capable of halting the malicious activity. Logging permits the malicious activity to be further analysed and used for network forensics. The criteria that was used to evaluate this were if the attacks carried out were logged, and if the logs were extractable. Agnitium Outpost, Blackice, Comodo, Sunbelt Keiro and ZoneAlarm logged the Nessus and nmap attacks. However, of these five personal firewalls, ZoneAlarm was the only application which does not permit the extraction of the logs into an easy to analyse format. Although Norton did not detect the attacks, it does permit logs to be easily extracted for future forensics.

Table 4 Firewall vulnerability comparison when using bitTorrent application

Firewall Software	Standalone Firewall		Firewall with bitTorrent	
	p0f::	nmap 3.75::	p0f::	nmap 3.75::
Agnitiun Outpost Firewall	✓	✘	✓	✘
Armor2net	✓	✓	✓	✓
Blackice	✓	✘	✓	✘
Comodo Personal Firewall	✓	✘	✓	✘
Keiro WinRoute Firewall	✓	✓	✓	✓
Norton Personal Firewall 2006	✓	✓	✓	✓
Panda Antivirus + Firewall 2007	✓	✘	✓	✘
Sunbelt Keiro Personal Firewall	✓	✘	✓	✘
Tiny Personal Firewall 2005	✓	✓	✓	✓
Zonelabs ZoneAlarm Free	✓	✘	✓	✓

Table 5: Firewall performance evaluation

Firewall Software	Detection (Alerting)		Response (Block fully)		Logging	
	Nessus	nmap	Nessus	nmap	Logged	Extractable
Agnitiun Outpost Firewall	✓	✘	✘	✓	✓	✓
Armor2net	✓	✓	✘	✓	✘	✘
Blackice	✓	✓	✘	✓	✓	✓
Comodo Personal Firewall	✓	✓	✓	✓	✓	✓
Keiro WinRoute Firewall	✘	✓	✘	✓	✘	✘
Norton Personal Firewall 2006	✓	✘	✘	✘	✘	✓
Panda Firewall 2007	✓	✓	✘	✓	✘	✘
Sunbelt Keiro Personal Firewall	✘	✓	✓	✓	✓	✓
Tiny Personal Firewall 2005	✘	✘	✘	✘	✘	✘
Zonelabs ZoneAlarm Free	✓	✓	✘	✓	✓	✘

Ability to update

The ability to update component of the evaluation investigated the complexity an end-user may face in updating the firewall application(Table 6). The analysis was performed by analysing how updates are instantiated on the personal firewall. Tiny Personal and Blackice were the only firewalls which did not automatically update the application at pre-defined intervals via a schedule. Norton and Armor2net did not incorporate a manual ‘check’ and ‘download’ function. Simplicity was determined by investigating what was required in order for the update to proceed. Most of the firewalls updated in the background and hence do not require input from the end-user.

However, Blackice updates by downloading an 'updater.exe' file to the end-users computer. When the file is run, Blackice itself detects that the file is malicious and does not recommend it be run. ZoneAlarm in a similar fashion requires that a completely new installation package be downloaded. The end-user must then uninstall the previous version before attempting to re-install the latest product version.

Table 6: Complexity of the update process for a range of personal firewall products

Firewall Software	Automatic	Manual	Simplicity
Agnitiun Outpost Firewall	✓	✓	Easy
Armor2net	✓	✘	Easy
Blackice	✓	✓	Difficult:: Downloads patch which is consider malicious by Blackice
Comodo Personal Firewall	✓	✓	Easy:: Requires system restart
Keiro WinRoute Firewall	✓	✓	Easy
Norton Personal Firewall 2006	✓	✘	Easy
Panda Firewall 2007	✓	✓	Easy
Sunbelt Keiro Personal Firewall	✓	✓	Easy
Tiny Personal Firewall 2005	✘	✓	Easy
Zonelabs ZoneAlarm Free	✓	✓	Difficult:: Requires re-download / re-installation

CONCLUSION

The research has successfully investigated the robustness of current popular personal and home use firewalls. Results from this study show that numerous personal firewalls are significantly behind in their overall level of security. Even though ZoneAlarm and Blackice are in the top of the market share, they are far from securing a system at the level as Comodo Personal Firewall. Tiny Personal Firewall is the only firewall which does not automatically check and attempt to download any necessary updates. This may leave an unsuspecting individual vulnerable especially if they do not manually check for updates over a long period of time. Furthermore, the difficulty in updating the Zonelabs ZoneAlarm firewall may deter individuals from updating their product, or leave them vulnerable while they uninstall the previous outdated version.

One of the elements manufactures appear to be focusing on is colourful backgrounds and sounds which may be personally configured through the interchangeable firewall application schemes. However, evidence from this research suggests that firewall developers must focus on securing systems from passive attacks such as those carried out by p0f. None of the firewalls tested detected any presence of any passive operating system fingerprint monitoring. Once the operating is detected, exploits can be found on the Internet with ease and used to cause havoc on an unsuspecting victim's computer system. A simple search through popular search engines can easily discover various attacks which can be carried out on an operating over a network.

Further research is necessary to determine if the Windows firewall when enabled does in fact interfere with third party firewalls and/or is there any increase or decrease in the level of system security. Further testing of firewalls using various utilities may also further investigate and determine the strength of firewalls and identify if the Comodo Personal Firewall which appears as the currently recommend firewall can withstand further penetration testing.

REFERENCES

Boeckeler, M. C. (2004) Overview of Security Issues Facing Computer Users, URL http://www.sans.org/reading_room/whitepapers/awareness/1399.php?portal=44896a03c8b1d3372685c8f67e5ffe51, Accessed 16 September 2006

Droppleman, R. (2004) Maintaining a Secure Network, URL http://www.sans.org/reading_room/papers/download.php?id=1445&c=ddac086f4603c4434b5a554e87641056, Accessed 16 September 2006

Fan, W., Miller, M., Stolfo, S., Lee, W., & Chan, P. (2004) Using artificial anomalies to detect unknown and known network intrusions, Knowledge and Information Systems, 6, 507-527.

Frisk, U., & Drocic, S. (2004) The State of Home Computer Security. Linkopings University, Linkoping, Sweden.

Markus, H. S. (2006) Personal Firewall Reviews, URL http://www.firewallguide.com/software.htm, Accessed 15 September 2006

PCWorld. (2005) Top Firewalls: Prevent Breaches, Upgrade What You Already Have, URL http://www.pcworld.com/downloads/collection/collid,59-order,1-c,downloads/files.html, Accessed 15 September 2006

Seshardi, A., Luk, M., Perrig, A., Doorn, L. V., & Khosla, P. (2006) Externally Verifiable Code Execution, Communications of the ACM, 49(9), 45-49.

Warkentin, M., Luo, X., & Templeton, G. F. (2005) A Framework for Spyware Assessment, Communications of the ACM, 48(8), 79-84.

West, R. (2006) HCI and security: Introduction. Interactions, 13(3), 18-19.

Yee, J. (2002). Firewall or FireFolly - An initial investigation into the effectiveness of Personal Firewalls in securing personal computers from attack, In 2002 Australian Information Warfare and Security Conference, Perth, Western Australia.

COPYRIGHT