The 2009 Personal Firewall Robustness Evaluation

Ken Pydayya, Peter Hannay & Patryk Szewczyk
secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University

Abstract

The evolution of the internet as a platform for commerce, banking, general information and personal communications has resulted in a situation where many individuals who may not have previously required internet access now require this connectivity as part of their everyday lives. In addition to this the widespread adoption of mobile broadband has lead to an increasing number of individuals having public facing IP addresses with no firewall appliances present. This situation has dramatically increased reliance on personal firewalls as the first and often last defence against intruders (human and malware alike). The evaluation performed demonstrates the capabilities of current personal firewall software to mitigate the threat posed by these intruders. The results show that the majority of personal firewall products evaluated are somewhat effective in reducing the risks remote exploitation but leave something to be desired in the area of information disclosure.

Keywords

Personal firewall; software firewalls; testing; evaluation; nmap; nessus; penetration testing.

INTRODUCTION

As the Internet evolves individuals who may not have previously required access to online resources are now conveniently acquiring products and services via the Internet (Szewczyk & Furnell, 2009). These same individuals, who are acquiring products via the Internet, often do not understand nor have the expertise to implement sufficient security onto their workstation. In-turn attackers are exploiting the novice Internet users' skill set, to acquire personal and confidential information from unsuspecting victims. This is evident in that many novice computers users are unable to differentiate between legitimate and phishing emails, or firewalls and anti-virus software (Dodge, Carver, & Ferguson, 2007).

Anti-virus products provide an avenue of defence to the average Internet user in that malicious software may be detected and removed in a timely manner. However, had the anti-virus product not detected a newly released malware then the victims machine is susceptible to a range of threats. Fortunately new malware tends to steer away from traditional malicious activities such as corrupting or deleting data on the workstation. Instead, malware may transform the workstation to a zombie in a collection of botnets, to further target and attack vulnerable hosts (Schultz, 2006). Whilst there isn't one solution for diminishing the risk of botnets, there are methods by which to limit or control the amount of damage caused. A botnet requires an open Internet connection to connect and communicate with its controller and vulnerable hosts. Hence, an updated and well configured firewall may halt the botnets connection, and in-turn prevents the vulnerable host from participating and attacking other hosts.

Many consumers attempt to implement a solution onto their workstation to prevent malicious activity from occurring. Unfortunately many end-users do not have the skill set to evaluate and determine best possible security tools for their workstation. In a recent study many consumers reported utilising a product that was marketed in a clever and convincing manner (Szewczyk & Furnell, 2009). To this, many respondents felt that Norton Anti-virus or Norton Firewall, was a suitable security product for their computer. The main reason for this judgement was that a trial version of the product came pre-installed on their newly purchased workstation and as a result they continued to use it as it appeared never required user interaction. Alternatively, respondents also claimed that Norton had advertised its product on both television and online. In-turn respondents could name only one company who developed security products. The impact of this, is that Norton is not only the most expensive security product on the market, but furthermore it does not rank as being one of the most effective security products according to third party evaluations (Best Firewall Software, 2009; Personal Firewall Software Review, 2009).

The effectiveness of a personal firewall is subject to its ability to effectively control and block incoming and outgoing traffic. In addition software firewalls operate through a learning process in which programs and processes may be allowed or denied access to the Internet. If a new process is executed on the selected workstation which requires Internet access, the firewall should continually block access until the end-user clearly permits the traffic to flow. Unfortunately software firewalls do not clearly and legibly present information on the programs or process which are attempting to access the Internet. As a result numerous end-users tend to remove or uninstall the firewall as the questions the firewall

presents are often not aimed at an individual with little or no expertise in computer or network security (Frisk & Drocic, 2004).

The effectiveness of a firewall may rapidly change. As new flaws are detected a firewall which was once considered ideal, could quickly become flawed and vulnerable. A vulnerability within a firewall is an error which is prominent in the design, development and configuration phase (Kamara, Fahmy, Schultz, Kerschbaum, & Frantzen, 2003). Vendors continually release updates for their firewall products, however these updates usually require user interaction which may deter the end-user from applying the update. Vulnerabilities within a firewall may lead to the exploitation of further vulnerabilities in the operating system and installed software, leaving the end-user susceptible to a range of threats.

In 2006 an unbiased evaluation was conducted on the top ten personal firewalls at the time as rated by numerous independent sources (Szewczyk & Valli, 2006). The top ten firewalls were taken from two independent websites and tested utilising a variety of penetration testing methods. Furthermore, the firewalls were also examined for their user friendliness and their initial configuration. The previous research identified that a test system utilising Comodo Personal Firewall resulted in the least number of vulnerabilities or open ports. Its ability to self update was flawless, and there was a vast amount of tutorials and instructions provided to the end-user. It also ranked both first and second amongst the independent reviews of personal firewalls taken at that time.

Over the duration of the last three years vendors have continued to release updates and revised versions of their products. As a result the top ten software firewall has changed. Utilising similar network penetration methods, the firewalls were examined for their ability to with stand tests based on and updated network attacks.

METHOD

The test systems comprised of two PC clone systems interconnected within a private network. Each system was utilising a Microsoft Windows XP Professional operating system with Service Pack 2 installed and all the latest patches and updates up to and including April 10th, 2009. Each firewall was independently installed on the test system using didactic recommendations made by the vendors through the installation and configuration process.

Table 1 - Personal Firewalls tested

Product	**Version**
AVG Anti-Virus Plus Firewall	8.5
eConceal Firewall Pro	2.0.019.1
Norman Personal Firewall	7.10.1200
Outpost Firewall	6.5.2358
Sunbelt Personal Firewall	4.6.1861.0
Sygate Personal Firewall	5.6.2802
Tiny Firewall	6.5.92
Webroot Desktop Firewall	5.8.0.25
ZoneAlarm Pro Firewall	7.0.470.000
Windows Firewall	-

Each system was tested with one of the listed firewalls with a series of known and published exploits that a competent firewall should be able to stop. A brute force of the system was undertaken by Tenable Nessus 3.2.1.1 with all of the vulnerability assessment plug-ins enabled. An assessment of open and vulnerable ports was undertaken via Nmap, and a Windows based security tested conducted by Manage Engine Security Manager Plus V5.0.

In each situation the software was tested with the default settings enabled, in the instance that a setup selection was required, the highest (purportedly most secure) setting was chosen. The justification for this is that it will provide a balanced scenario for the evaluation of each firewall, in addition the default selection emulates the behaviour of a large proportion of users.

The network scanners were launched against each firewall in sequence. In order to simulate user activity the default option was chosen in the case of prompts by the personal firewall software. On the completion of each scan the results were recorded for each port. As a baseline the system was scanned with no personal firewall present. These baseline results are provided in each result set for comparative purposes.

RESULTS

Prior to the commencement of the testing process the open ports on the system were evaluated in order to determine the baseline for testing purposes. In this case the results of the baseline test are shown alongside the results in Figure 1. The examination of these results shows clearly that each of the firewall utilities performed differently against the varying scan types used by each port scanner. In this case the only firewall software which did not leave any ports accessible was the in-built windows firewall. It should be noted however that a port being simply accessible does not necessarily pose a security risk or represent vulnerability. The presence of an open port only demonstrates that it is possible to communicate with an application listening on that specific port.

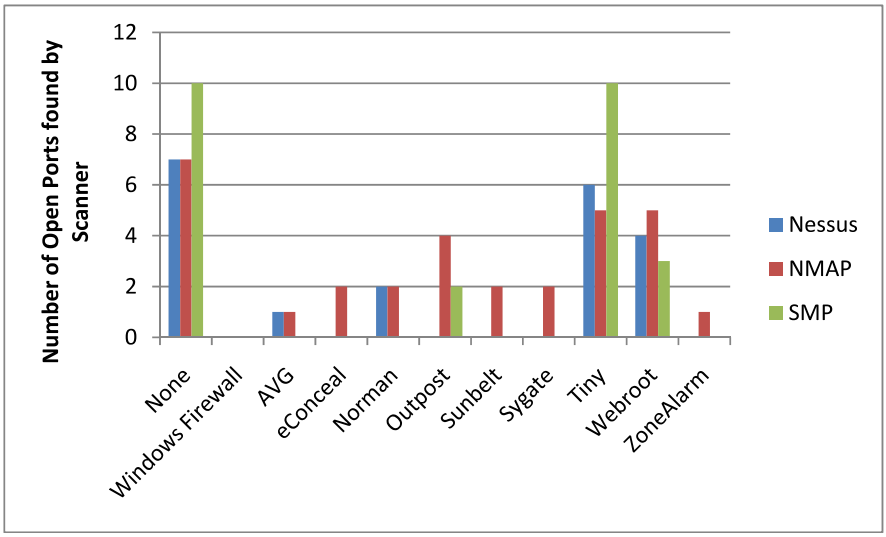

Figure 1 - Firewall Performance by Open Ports Detected

The results of the complete Nessus vulnerability scan are shown in the figure 2 below. In these scan results the risk associated with each vulnerability has been broken down into three categories: low, medium and high. The risk evaluations were provided by the Nessus software itself, with low risk representing a non-serious information disclosure, such as the system time. Medium risk represents information disclosure that may be serious, such as installed applications. Finally high risk signifies the presence of a vulnerability that may allow an attacker to interrupt the operation of the system or execute custom commands / code.

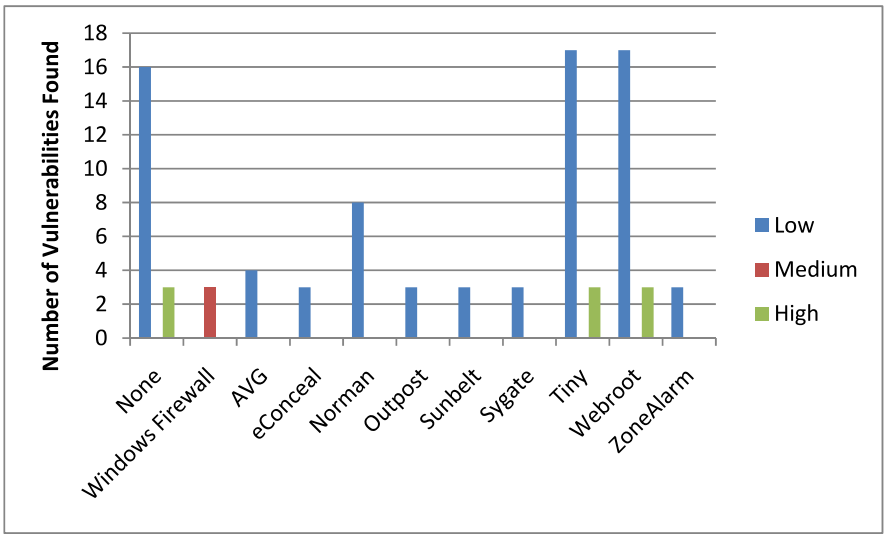

Figure 2 - Firewall Performance by Vulnerabilities Detected

As demonstrated in figure 2 there were no products which did not allow any information disclosure, however this in itself may not pose a significant security threat. The results are fairly positive for the majority of personal firewalls protecting against medium/high classed risks. The personal firewalls which did not shield against risks classified as medium or high are: Windows Firewall, Tiny Firewall and Webroot Desktop Firewall. It is also worth noting that Tiny Firewall and Webroot Desktop Firewall allowed for information disclosure that was not possible with no firewall present.

CONCLUSION

The importance of robust personal firewall software is rapidly becoming more critical as the adoption of mobile broadband and commercial wireless services increase. The increase in uptake of these services can be likened to the past in which dialup modems we're common, as in both of these scenarios internet access is often direct, with the computer being assigned a publicly accessible IP address. This situation results in the direct exposure of users to network aware malware on the internet, without the need to compromise NAT filtering which has previously protected home users to a limited extent.

The research has successfully investigated the robustness of a number of personal firewall products. The results of this research demonstrate that the majority of personal firewall products tested provides a significant level of protection when tested in the defined manner. It is of interest however that two of the personal firewall products tested allowed for additional information disclosure that was not present with no firewall installed. The nature of this information disclosure warrants further research.

REFERENCES

Best Firewall Software. (2009). Best Firewall Software - Editor's Choice. Retrieved July 9, 2009, from http://www.all-internet-security.com/top_10_firewall_software.html

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

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

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., & Frantzen, M. (2003). Analysis of vulnerabilities in Internet firewalls. *Computers & Security, 22*(3), 214-232.

Personal Firewall Software Review. (2009). 2009 Personal Firewall Software Review Product Comparisons. Retrieved June, 15, 2009, from http://personal-firewall-software-review.toptenreviews.com/

Schultz, E. (2006). Where have the worms and viruses gone?—new trends in malware. *Computer Fraud & Security, 2006*(7), 4-8.

Szewczyk, P., & Furnell, S. (2009). *Assessing the online security awareness of Australian Internet users.* Paper presented at the 8th Annual Security Conference, Las Vegas, NV.

Szewczyk, P., & Valli, C. (2006). *Personal Firewalls – Testing Robustness.* Paper presented at the 4th Australian Information Security Management Conference Edith Cowan University, Mt Lawley, Western Australia.

APPENDIX A

Port scan results for each scanner & personal firewall.

	NESSUS (Inbuilt Port Scanner, Default Settings)											
	ICMP	UDP							TCP			
Product	N/A	123	137	138	445	500	1900	4500	21	135	139	445
None	X	X	X		X					X	X	X
Windows Firewall												
AVG		X										
eConceal												
Norman	X	X										
Outpost												
Sunbelt												
Sygate												

Tiny	X	X	X							X	X	X
Webroot	X	X									X	X
ZoneAlarm												

	NMAP (Connect, SYN & UDP)											
	ICMP	UDP							TCP			
Product	N/A	123	137	138	445	500	1900	4500	21	135	139	445
None	X	X	X		X					X	X	X
Windows Firewall												
AVG									X			
eConceal	X								X			
Norman	X								X			
Outpost	X								X		X	X
Sunbelt	X								X			
Sygate	X								X			
Tiny	X								X	X	X	X
Webroot	X								X	X	X	X
ZoneAlarm									X			

	SMP											
	ICMP	UDP							TCP			
Product	N/A	123	137	138	445	500	1900	4500	21	135	139	445
None		X	X	X	X	X	X	X		X	X	X
Windows Firewall												
AVG												
eConceal												
Norman												
Outpost											X	X
Sunbelt												
Sygate												
Tiny		X	X	X	X	X	X	X		X	X	X
Webroot										X	X	X
ZoneAlarm												

COPYRIGHT