2010

The 2010 Personal Firewall Robustness Evaluation

Satnam Singh Bhamra
Edith Cowan University

DOI: 10.4225/75/57b28f7240cd6
Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

The 2010 Personal Firewall Robustness Evaluation

Satnam Singh Bhamra
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
s.bhamra@ecu.edu.au

Abstract
With the advent of cheaper Internet connections, the number of Internet connections among home users is on the rise. Generally, home users have little understanding of the security concerns associated with Internet connectivity. To protect against computer attacks, generally a home user may install a personal firewall on his/her computer. To determine the effectiveness of personal firewalls, evaluation tests were performed against the ten firewall products available to users at local electronic stores and listed on popular firewall security websites. The firewalls were tested in their default and maximum security mode. The investigation was carried out by performing a port scan and vulnerability scan attacks against a computer with no firewall protection and computers running personal firewalls. The results of the investigation established that the computers running the firewalls exhibited some or all of the vulnerabilities detected on a computer with no firewall protection.

Keywords
Personal firewall testing, vulnerability testing, openvas, nessus, nmap.

INTRODUCTION

The acceptance of the Internet comes at a cost. An Internet connection opens a gateway for an unauthorised public audience to exploit private information stored on private hosts. Private or Public corporations generally have the financial backing and expertise staff, to stay protected against these exploits. However, home users are typically computer security illiterate, and often are left vulnerable to computer attacks. There are countless public and private resources available to home users, to educate them on how to protect themselves on the Internet. Public examples of such a resource are two websites launched by the Australian Government, www.cybersmart.gov.au and www.staysmartonline.gov.au. These websites are designed to guide home users, on the security challenges of the Internet, and the precautions they can take against these challenges. The use of a personal or desktop firewall on computer connected to the Internet is recommended on these websites.

Several firewall vendors over the past few years have started to develop free and/or affordable personal firewall applications for home users (Herzogl & Shahmehri, 2007; McDermott, 2000; McDougall, 2001). Operating systems developers such as Microsoft and Apple have also started to include a built-in personal firewall into their OS (NYU, 2006). A personal firewall is a software-based firewall security suite, designed for those with limited computer networking and security skills (Raja, Hawkey, Beznosov, & Booth, 2010), which is installed on a single computer, and provides security protection against threats for only that system (Whelan, 2006).

Personal firewalls work by controlling and monitoring inbound and outbound connections on a computer based on a firewall policy, which may be pre or user defined (Cieslak, 2006). It can monitor and control not only network layer traffic, but also application layer traffic (Felman, 2004). In addition to these firewall features, many of the current personal firewalls also include anti-virus protection, malware protection, ad-filtering and email attachment filtering capabilities (Cieslak, 2006).

A personal firewall can be used by home users as a security layer against security attacks. However, previous research has demonstrated that in various instances a personal firewall fails to protect a system from known security attacks (Herzogl & Shahmehri, 2007; Pydayya, Hannay, & Szewczyk, 2009; Szewczyk & Valli, 2006; Yee, 2002). This study builds upon the previous personal firewall research, by investigating the effectiveness of personal firewall products available in 2010 on a Windows 7 machine.

METHOD

Personal firewalls in theory stealth a computer from network scan attacks. The objective of this study was to evaluate how personal firewalls respond to a (1) port scan and (2) vulnerability scan attacks.

The test environment comprised of two virtual machines (1) Windows 7 for housing the personal firewalls and (2) Backtrack 4 for running Nmap, Nessus 4.2.2 and OpenVAS 2.0.2 scanners. To select the firewall products to be tested, products those are available to the local consumers at local computer stores such as JB HI-FI, Dick Smith and Officeworks and the top-rated personal firewalls listed on "firewallguide.com", were chosen for the study. The default and maximum security level for each firewall was investigated, and Table 1 lists the personal firewall products used in this research.

Product Name	Version
Comodo Firewall	4.1.150349.920
ESET Smart Security 4	4.2.40.0
F-Secure Internet Security 2010	10.00 Build 246
Kaspersky Internet Security 2010	9.0.0.736
McAfee Internet Security 2011	11.5
Norton Internet Security 2010	17.8.0.5
Outpost Firewall Pro 7.0	3373.514.1234
Trend Internet Security 2011	17.50.1647.0000
Windows Firewall	Windows 7 Home Premium Built-in Firewall
ZoneAlarm Free Firewall	9.2.057.000

Table 1 - Name of the Personal Firewall Products Tested

To define a benchmark for evaluating the testing results, a Windows 7 machine with no firewall was tested, and its results set the baseline for the evaluation process.

DISCUSSION

Data collected in the testing stages, points to the fact, that machines loaded with the firewalls displayed some weaknesses. Some firewalls, to a certain extent, managed to shield the computer from the attacking probes. In this section, the findings of the Nmap, vulnerability scanning and other relevant data discovered as part of the research will be discussed.

NMAP RESULTS DISCUSSION

In theory personal firewalls stealth's open ports, and protects and alerts against port scan attacks. Unfortunately, when this is put into practice, the results are undesirable. The baseline machine returned thirteen open ports.

Default firewall security level findings: From the overview presented in Table 2, one can identify:

1. Only two firewalls out of the ten tested, blocked the address of the Nmap attacker. These were ESET and Outpost firewalls. Outpost temporary blocked the attacker for 5 minutes, while ESET didn't display the blockage time.

2. Only three firewalls produced an alert upon the detection of the Nmap attack. The failure of other ten firewalls to alert, indicates a user may not be aware of an attack happening.

3. Only six firewalls logged the Nmap attack. Of these six firewalls, ESET, F-Secure, McAfee and Kaspersky logged the attack as a type of port scan attack. Norton logged it as an intrusion attempt attack, without defining what the intrusion attempt was. Outpost logged the Nmap attack as a scan, without explaining the term scan.

4. ESET firewall provided the best protection against the Nmap attack. ESET logged the Nmap scan, and temporarily blocked the attacker. This resulted in Nmap detecting no open ports, which indicates the likelihood of exploiting the machine via a port is significantly low. The only downside of the ESET firewall was it failed to produce an alert upon the detection of the Nmap attack.

5. Outpost firewall offered the second best protection against the Nmap attack. Outpost logged and alerted on the scan, and also temporarily blocked the attacker.

6. The Nmap scan against Comodo and Windows Firewall machines returned similar results, and significantly fewer open ports than the baseline. The downsides of these firewalls were none of them alerted about the Nmap scan or blocked the attacker. By default logging is disabled on Windows Firewall. This means, Windows Firewall doesn't keep a record of incoming and outgoing traffic. Comodo firewall has logging enabled, but it failed to log the attack or produce an alert and, also block the Nmap attacker.

7. Norton firewall returned seven open ports. Norton firewall detected the Nmap attack, but didn't produce an alert. F-Secure firewall returned ten open ports. F-Secure detected and produced an alert message for the Nmap attack.

8. The Nmap scan against the machines running Trend Micro and ZoneAlarm firewalls returned similar results as the baseline. Both firewalls didn't detect/log or alert on Nmap attack. This means the installation of Trend Micro and ZoneAlarm failed to protect the machine against the port scan attack.

9. The machine running Kaspersky firewall returned more open ports than the baseline. This is because Kaspersky opened two extra ports, 1110 and 19780, for its operation. These extra ports may add weakness to the machine, as a hacker may try to exploit them, and this may not be the case on the baseline machine. Kaspersky firewall detected and alerted on the Nmap scan. The alert message had interesting information in it. The alert message indicated, Kaspersky has detected an attack, but the attacker address was not blocked, because it could be spoofed.

Maximum firewall security level findings: From the overview presented in Table 3, one can identify:

1. Windows Firewall doesn't provide an option to increase the level of security. This means, it is limited to default security mode.

2. The Nmap scan for the machines running McAfee, Comodo, Outpost, F-Secure, ESET and Norton firewall, returned no open ports. This is because, in the maximum firewall security mode, these firewalls block all uninitiated incoming traffic.

3. Outpost and Kaspersky were the only firewalls to produce an alert upon the detection of the Nmap attack, and to log the attack. Outpost firewall temporarily blocked the Nmap attacker for 5 minutes.

4. Only three of the ten firewalls running in the maximum state, returned open ports:

    i. The machine running ZoneAlarm firewall returned three open ports. In its default mode, ZoneAlarm didn't detect or alert on the incoming Nmap attack, and the same applied when it was running in maximum security mode.

    ii. The machine running Kaspersky firewall returned eight open ports. Kaspersky detected an alert on the incoming Nmap attack. Kaspersky failed to block the attack, because according to the Kaspersky firewall, the source of the attack could be spoofed, so it would not be blocked. This was the same behaviour when Kaspersky was running in the default security mode.

    iii. The machine running Trend Micro firewall in its maximum security state returned more ports than its default security state. Nmap detected thirteen open ports, and one closed port. A closed port is a port which can send and receive packets, but there is no application/service attached to it. The port detected as closed was 554, the Windows media server port. This port was detected open, when Trend Micro was running in default mode. Nmap also detected a new port, which was detected by Nmap when Trend Micro was running in default mode. The new port detected was 5357, the Microsoft network discovery port. In its default mode, Trend Micro didn't detect or alert on the incoming Nmap attack, and the same applied when it was running in maximum security mode.

Product	Open Ports	Nmap Alert	Nmap Logging	Logged As	Attacker Blocked	Summary
ESET Smart Security 4	0	No	Yes	Port Scanning Attack	Yes	ESET offered the best protection against the Nmap attack. It stealth all open ports detected under the baseline machine.
Outpost Firewall Pro 7.0	2	Yes	Yes	Scan	Yes	It alerts on the Nmap attack and logs it. Upon detection of the Nmap attack, it blocked the source of the attack.
Windows Firewall	3	No	No	NA	No	Logging is disabled by default. The firewall doesn't produce alerts. The firewall doesn't display if it blocks the attack, and there is no option to confirm this. But it managed to stealth some open ports which were detected under the baseline scan.
Comodo Firewall	3	No	No	NA	No	It doesn't log or alert on the Nmap scan. It does stealth some open ports, as it returns significantly lower number of open ports than the baseline.
Norton Internet Security 2010	7	No	Yes	Intrusion Attempt	No	It logs the attack, but doesn't produce an alert, which means the user may not be aware of the attack. It manages to stealth some open ports which were detected under the baseline scan.
F-Secure Internet Security 2010	10	Yes	Yes	Nmap Scan	No	It logs and alerts on the Nmap scan. It also manages to stealth some open ports, which were detected under the baseline scan.
McAfee Internet Security 2011	10	No	Yes	TCP Port Scan	No	It logs the attack, but it doesn't produce an alert. McAfee also opens a new port for its operation, which doesn't appear on the baseline machine.
ZoneAlarm Free Firewall	13	No	No	NA	No	It doesn't log or alert on the Nmap scan. It doesn't stealth open ports, as it returns the same number of ports as the baseline scan.
Trend Internet Security 2011	13	No	No	NA	No	It doesn't log or alert on the Nmap scan. It doesn't stealth open ports, as it returns the same number of ports as the baseline scan.
Kaspersky Internet Security 2010	15	Yes	Yes	Network Attack Scan	No	It returned more open ports than the baseline machine. This is because Kaspersky opened two extra ports. These extra ports add weakness to the system, as the hacker may try to exploit them, and this may not be case on the baseline. Kaspersky also failed to block the attack, because according to it the origin of the attack may be spoofed. This raises security concerns, as the attack origin may not be spoofed.

Table 2 - Nmap Scan Summary for the Personal Firewalls Running in Default Security Mode

Product	Open Ports	Nmap Alert	Nmap Logging	Logged As	Attacker Blocked	Summary
Windows Firewall	NA	NA	NA	NA	NA	Windows Firewall doesn't offer an option to increase its firewall protection level.
Norton Internet Security 2010	0	No	No	NA	No	Norton blocked all incoming traffic in the maximum security state. Like its default state, It didn't alert on the Nmap scan.
ESET Smart Security 4	0	No	Yes	Port Scanning Attack	Yes	ESET blocked all incoming traffic in the maximum security state, but it managed to detect the attack and log it.
F-Secure Internet Security 2010	0	No	No	NA		F-Secure blocked all incoming traffic in the maximum security state.
Outpost Firewall Pro 7.0	0	Yes	Yes	Scan	Yes	Outpost blocked all incoming traffic in the maximum security state. It detected the attack, produced an alert and logged it.
Comodo Firewall	0	No	No	NA	No	Comodo blocked all incoming traffic in the maximum security state. Like its default state, It didn't detect or alert on the Nmap scan.
McAfee Internet Security 2011	0	No	No	NA	No	McAfee blocked all incoming traffic in the maximum security state. Like its default state, It didn't alert on the Nmap scan.
ZoneAlarm Free Firewall	3	No	No	NA	No	Like its default state, it didn't detect or alert on the Nmap scan. It does stealth open ports, as it returned fewer ports than the port scan output of its default state.
Kaspersky Internet Security 2010	8	Yes	Yes	Network Attack Scan	No	Kaspersky managed to stealth some open ports, which were detected open by Nmap when it was running in default state. Kaspersky failed to block the Nmap scan, just like when it was operating in its default state.
Trend Internet Security 2011	14	No	No	NA	No	Nmap scan of Trend Micro running in maximum security state detected one extra port. This port was the 5357, which was detected in its default security mode. Like its default state, it didn't detect or alert on the Nmap scan.

Table 3 - Nmap Scan Summary for the Personal Firewalls Running in Maximum Security Mode

VULNERABILITY RESULT DISCUSSION

The goal of the vulnerability scan was finding out if the personal firewalls are able to hide software vulnerabilities for Windows 7. Two different vulnerability scanners were used:

1. OpenVAS: An open source vulnerability scanner.
2. Nessus: The free version of Nessus.

Nessus Results Discussion

Nessus scanner organises detected vulnerabilities into four different risk categories: low, medium, high and critical. The Nessus scanner only detected low severity vulnerabilities on the baseline and machines running the personal firewalls. The Nessus scan of the baseline machine returned twenty-five vulnerabilities.

Default firewall security level findings: From the overview presented in Table 4, one can identify:

1. Only Outpost and ESET firewalls managed to block the source of the Nessus scan.

2. Only Outpost and Kaspersky firewalls produced an alert upon the detection of the Nessus scan. The failure of other ten firewalls to alert indicates a user may not be aware of a vulnerability scan happening against his/her computer.

3. Only five firewalls logged the Nessus scan. Of these five firewalls, McAfee and ESET detected it as a port scan attack, and Kaspersky detected it as a network attack scan. Norton detected it as an intrusion attempt, without defining what the intrusion was. Outpost detected it as a MOYARI13 attack. Outpost doesn't provide any help in its log window to explain what a MOYARI13 attack is.

4. Only one firewall out of the ten tested, completely protected the computer from the Nessus scan. This was the Norton firewall. This indicates the likelihood of exploiting a known vulnerability is significantly low on the machine running the Norton firewall. Norton detected and logged the Nessus scan, but failed to produce an alert.

5. The machine running ZoneAlarm firewall returned similar results as the baseline. ZoneAlarm firewall failed to detect, log and block the Nessus scan.

6. The machine running ESET firewall returned sixteen vulnerabilities. ESET detected the scan, but failed to log it.

7. The machine running Trend Micro firewall returned one less vulnerability than the baseline. The vulnerability missing was the plugin ID 10114, which is for the ICMP Timestamp Request Remote Data Disclosure. Trend Micro failed to detect, log and block the Nessus scan.

8. The machine running Kaspersky firewall returned an additional vulnerability than the baseline. This is because of the Kaspersky custom port 1110. Kaspersky detects and logs the Nessus scan. It failed to block the Nessus scan, for the same reason as the Nmap attack.

Product	Number of Vulnerabilities	Nessus Alert	Nessus Logging	Logged As	Attacker Blocked	Summary
Norton Internet Security 2010	1	No	Yes	Intrusion Attempt	No	The only detected vulnerability by Nessus was the plugin id 35716.
F-Secure Internet Security 2010	7	No	No	No	No	Significantly lower number of vulnerabilities than the baseline machine. F-Secure failed to detect, log and block the origin of the scan.
Outpost Firewall Pro 7.0	9	Yes	Yes	Moyari13	Yes	Alert upon the detection of the Nessus scan and logged it. Outpost logged the Nessus scan as a MOYARI13 attack, without any explanation of a MOYARI13 attack.
McAfee Internet Security 2011	10	No	Yes	TCP Port Scan	No	Detected and logged the Nessus scan as a port scan attack. The machine running McAfee displayed significantly lower number of vulnerabilities than the baseline machine.
ESET Smart Security 4	16	No	Yes	Port Scanning Attack	Yes	Detected the Nessus scan and temporarily blocked the attacker. Even though the attacker was blocked, the machine running ESET retuned sixteen vulnerabilities. It logged the Nessus scan as a port scan attack.
Windows Firewall	20	No	No	NA	No	By default logging is disabled, therefore it doesn't detect or the log the scan.
Comodo Firewall	20	No	No	NA	No	It failed to detect the Nessus scan.
Trend Internet Security 2011	24	No	No	NA	No	It failed to detect or block the Nessus scan. The machine running Trend Micro returned one less vulnerability than the baseline. The missing vulnerability was the ICMP Timestamp Request Remote Data Disclosure.
ZoneAlarm Free Firewall	25	No	No	NA	No	It failed to detect or log the Nessus scan. The machine running the ZoneAlarm retuned the same number vulnerabilities as the baseline. This indicates ZoneAlarm failed to stealth the vulnerabilities detected in the baseline.
Kaspersky Internet Security 2010	26	Yes	Yes	Network Attack Scan	No	The machine running Kaspersky returned a higher number of vulnerabilities than the baseline. This was because of the proprietary ports Kaspersky for its operation. It failed to block the Nessus scan, because according to Kaspersky the attack origin may be spoofed.

Table 4 - Nessus Scan Summary for the Personal Firewalls Running in Default Security Mode

Maximum firewall security level findings: From the overview presented in Table 5, one can identify:

1. Only Outpost and ESET firewalls temporarily blocked the Nessus attacker.

2. Only Outpost, Kaspersky and ESET detected and logged the Nessus scan. Outpost and Kaspersky produced an alert upon the detection of the Nessus scan. ESET and Kaspersky logged the Nessus scan with the same name the firewalls did under their default mode. On the other hand, Outpost logged the Nessus scan with a different name from its default mode. Outpost logged it as a scan attack.

3. Only the machines running McAfee, Comodo and ZoneAlarm returned no vulnerabilities.

4. Trend Micro and ESET returned similar results to their default state. This would indicate, increasing the level of firewall protection, made no difference in hiding the system's vulnerabilities.

5. The machines running Norton, Outpost and F-Secure firewalls returned a single vulnerability, and that was plugin id 25220. This plugin is used to identify the network card brand.

OpenVAS Results Discussion

OpenVAS scanner organises detected vulnerabilities into four different risk categories: security notes, security warnings, and security holes and critical. The OpenVAS scanner only detected security notes and warnings vulnerabilities on the baseline machine. The OpenVAS scan of the baseline machine returned seventeen security notes and three security warnings vulnerabilities.

Default firewall security level findings: From the overview presented in Table 6, one can identify:

1. Only Outpost and ESET firewalls managed to block the source of the OpenVAS scan.

2. Only Outpost and Kaspersky firewalls produced an alert upon the detection of the OpenVAS scan.

3. Only five firewalls logged the OpenVAS scan. ESET and McAfee logged it as a port scan attack and Kaspersky logged it as a network attack scan. Outpost logged it as a scan and Norton as an intrusion attempt.

4. The machine running Kaspersky returned more vulnerabilities than the baseline. It returned one extra security notes vulnerability which OpenVAS defined as certain scripts failed to complete in a defined timeout. According to OpenVAS report page, the firewall running on the system, may have detected the scan and blocked the scripts. There was no mention of the scripts that failed to run. The machine running Kaspersky also returned a security hole, which the baseline and machines running the other firewalls did not. This security hole had a CVE ID of CVE-2009-3103. This security hole was for the remote code-execution vulnerability in the protocol header for the Server Message Block (SMB) Negotiate Protocol Request.

5. Norton and ESET firewalls provided the best protection against the OpenVAS scan. The OpenVAS results for machines running these firewalls returned only two security notes vulnerabilities.

6. The machines running ZoneAlarm, Trend Micro and ZoneAlarm returned similar results as the baseline.

Product	Number of Vulnerabilities	Nessus Alert	Nessus Logging	Logged As	Attacker Blocked	Summary
Windows Firewall	NA	No	No	NA	No	Windows Firewall doesn't offer an option to increase its firewall protection level.
McAfee Internet Security 2011	0	No	No	NA	No	McAfee blocked all incoming traffic in the maximum security state.
Comodo Firewall	0	No	No	NA	No	Comodo blocked all incoming traffic in the maximum security state.
ZoneAlarm Free Firewall	0	No	No	NA	No	ZoneAlarm blocked all incoming traffic in the maximum security state.
Norton Internet Security 2010	1	No	No	NA	No	Norton blocked all incoming traffic in the maximum security state. The only vulnerability detected by the Nessus scan was plugin ID 35716, which is for identifying the network card.
Outpost Firewall Pro 7.0	1	Yes	Yes	Scan	Yes	Outpost blocked all incoming traffic in the maximum security state. It detected the attack, produced an alert and logged it. Unlike its default state that logged the Nessus scan as a MOYARI13 attack and its maximum state logged it as a scan attack.
F-Secure Internet Security 2010	1	No	No	No	No	F-Secure blocked all incoming traffic in the maximum security state.
Kaspersky Internet Security 2010	2	Yes	Yes	Network Attack Scan	No	Kaspersky alerted and logged the Nessus scan. It failed to block the attacker, because according to Kaspersky the attackers address may be spoofed, so it will not block the attacker address.
ESET Smart Security 4	16	No	Yes	Port Scanning Attack	Yes	It logged the Nessus scan, and temporary blocked the address. But Nessus returned similar results for ESET running in default and maximum state.
Trend Internet Security 2011	24	No	No	NA	No	Nessus returned similar results for Trend Micro running in default and maximum state. Like its default state, Trend Micro running maximum state failed to detect or log the Nessus scan.

Table 5 - Nessus Scan Summary for the Personal Firewalls Running in Maximum Security Mode

Product	Notes	Warning	Holes	VAS Alert	VAS Logging	Logged As	Attacker Blocked	Summary
Norton Internet Security 2010	2	0	0	No	Yes	Intrusion Attempt	No	Norton detected and logged the OpenVAS scan. OpenVAS scan of the Norton machine returned only two vulnerabilities; Traceroute information and OS fingerprints result.
ESET Smart Security 4	2	0	0	No	Yes	Port Scanning Attack	Yes	ESET detected, logged and temporarily blocked the OpenVAS attacker. OpenVAS scan of the ESET machine returned only two vulnerabilities; Traceroute information and OS fingerprint results.
Outpost Firewall Pro 7.0	3	0	0	Yes	Yes	Scan	Yes	Outpost detected, logged and temporarily blocked the OpenVAS attacker. OpenVAS scan of the Outpost machine returned only three vulnerabilities; Traceroute information, OS fingerprints result and SMB information.
F-Secure Internet Security 2010	3	0	0	No	No	No	No	F-Secure failed to detect, alert or log the OpenVAS scan. OpenVAS scan of the F-Secure machine returned only three vulnerabilities; Traceroute information, OS fingerprints result and Open ports detection.
McAfee Internet Security 2011	16	3	0	No	Yes	TCP Port Scan	No	McAfee detected and logged the OpenVAS scan. OpenVAS scan of the McAfee machine returned one less vulnerability than the baseline.
Comodo Firewall	16	3	0	No	No	NA	No	Comodo failed to detect, alert or log the OpenVAS scan. OpenVAS scan of the Comodo machine returned one less vulnerability than the baseline.
Windows Firewall	17	3	0	No	No	NA	No	Returned similar results to that of the baseline.
ZoneAlarm Free Firewall	17	3	0	No	No	NA	No	Returned similar results to that of the baseline.
Trend Internet Security 2011	17	3	0	No	No	NA	No	Returned similar results to that of the baseline.
Kaspersky Internet Security 2010	18	3	1	Yes	Yes	Network Attack Scan	No	Returned more vulnerabilities than the baseline. The machine running Kaspersky was the only to return a security hole. This security hole was for the protocol header for the SMB protocol.

Table 6 - OpenVAS Scan Summary for the Personal Firewalls Running in Default Security Mode

Maximum firewall security level findings: From the overview presented in Table 7, one can identify:

1. Only Outpost, Kaspersky and ESET detected and logged the OpenVAS scan. Outpost and Kaspersky produced an alert upon the detection of the OpenVAS scan.

2. Only Outpost and ESET temporarily blocked the OpenVAS attacker. Kaspersky failed to block the attacker, for the reason given for the Nmap and Nessus scan in the previous sections.

3. Comodo, ESET, F-Secure, Kaspersky, McAfee, Norton, Outpost and ZoneAlarm returned similar results. For machines running these firewalls, OpenVAS returned only two security notes: OS fingerprints result and Traceroute information.

4. The machine running Trend Micro returned similar results to its default state. This would indicate, increasing the level of Trend Micro firewall protection, made no difference in hiding the system's vulnerabilities.

CONCLUSION

This research demonstrated that machines running personal firewalls displayed weaknesses, when exposed to the security attacks. A machine with no firewall protection was tested, so that its results could be used as a baseline to compare results for the firewalls.

In some instances, an installation of firewall returned similar or more weaknesses than the baseline. The Kaspersky firewall was one such example, which returned more open ports and vulnerabilities than the baseline machine. In other cases, personal firewalls often provide an option to increase its level of security protection. This would indicate, if a home user were to increase the security level to the maximum, the personal firewall would offer better protections than its default state. The Trend Micro firewall failed this notion, as it returned similar results in both default and maximum state.

Vendor websites list alerting, logging and blocking of attacks as the key advantages of a personal firewall. Norton and Kaspersky firewalls were the only firewalls to log the conducted attacks, and Outpost and ESET firewalls to block the source of the attacks. F-Secure, Windows Firewall, Comodo, Trend Micro and ZoneAlarm firewalls failed to log the attacks.

The literature reviewed, displayed examples of similar discoveries made by researchers on previous versions of personal firewalls. This trend raises questions, on the standard of testing these products undergo, before being made public. If we were to look at the sale of electrical equipment in Australia, such equipment has to pass safety requirements set by standards such as the AS/NZZ 60950.1, before being sold to consumers. This assures consumers that the products are safe to install, operate and maintain. However, there is no standard or model to test the validity of a personal firewall product, before being made public. Therefore, a home user may not be aware of the weaknesses displayed by personal firewalls, and may assume by installing a personal firewall on his or her computer, the system is secure from attackers.

Product	Notes	Warning	Holes	VAS Alert	VAS Logging	Logged As	Attacker Blocked	Summary
Windows Firewall	NA	NA	NA	NA	NA	NA	No	Windows Firewall doesn't offer an option to increase its firewall protection level.
Comodo Firewall	2	0	0	No	No	NA	No	Comodo blocked all incoming traffic in the maximum security state.
ESET Smart Security 4	2	0	0	No	Yes	Port Scanning Attack	Yes	ESET blocked all incoming traffic in the maximum security state.
F-Secure Internet Security 2010	2	0	0	No	No	NA	No	F-Secure blocked all incoming traffic in the maximum security state.
Kaspersky Internet Security 2010	2	0	0	Yes	Yes	Network Attack Scan	No	Kaspersky blocked all incoming traffic in the maximum security state.
McAfee Internet Security 2011	2	0	0	No	No	NA	No	McAfee blocked all incoming traffic in the maximum security state.
Norton Internet Security 2010	2	0	0	No	No	NA	No	Norton blocked all incoming traffic in the maximum security state.
Outpost Firewall Pro 7.0	2	0	0	Yes	Yes	Scan	Yes	Outpost blocked all incoming traffic in the maximum security state.
ZoneAlarm Free Firewall	2	0	0	No	No	NA	No	ZoneAlarm blocked all incoming traffic in the maximum security state.
Trend Internet Security 2011	17	3	0	No	No	No	No	The machine running Trend Micro in maximum security mode, returned similar results to that of its default mode.

Table 7 - OpenVAS Scan Summary for the Personal Firewalls Running in MAX Security Mode

REFERENCES

Cieslak, D. (2006). Personal firewalls. CPA Technology Advisor, 16(4), 34.

Felman, F. (2004). Personal firewalls protect vulnerable PCs. Network World, 21(25), 75.

Herzogl, A., & Shahmehri, N. (2007). Usability and security of personal firewalls. New Approaches for Security, Privacy and Trust in Complex Environments, 232(2007), 37-48.

McDermott, P. (2000). Personal firewalls...One more step towards comprehensive security. Network Security, 2000(11), 11-14.

McDougall, B. (2001). Personal firewalls - Protecting the home internet user. Retrieved March, 2010, from http://www.sans.org/reading_room/whitepapers/firewalls/personal_firewalls_protecting_the_home_internet_user_799

NYU. (2006). Personal firewalls. Retrieved March, 2010, from http://www.nyu.edu/its/pubs/pdfs/personal_firewalls.pdf

Pydayya, K., Hannay, P., & Szewczyk, P. (2009). The 2009 personal firewall robustness evaluation. Paper presented at the 7th Australian Information Security Management Conference, Kings Perth Hotel, Western Australia.

Raja, F., Hawkey, K., Beznosov, K., & Booth, K. S. (2010). Investigating an appropriate design for personal firewalls. Paper presented at the 28th international Conference Extended Abstracts on Human Factors in Computing Systems, Atlanta.

Szewczyk, P., & Valli, C. (2006). Personal firewalls - Testing robustness Paper presented at the 4th Australian Digital Forensics Conference, Perth.

Whelan, K. (2006). The Whelan IT security report - Personal firewalls. Retrieved March, 2010, from http://www.itcsecurity.com/files/upload-folder/Personal%20Firewalls.pdf

Yee, J. (2002). Firewall or fireFolly - An initial investigation into the effectiveness of personal firewalls in securing personal computers from attack. Paper presented at the 3rd Australian Information Warfare and Security Conference Perth.