Auditing Perimeter Defenses in a Home Office Environment with D-Link Broadband Router and Kerio Personal Firewall – An Administrators Perspective

GSNA Practical Version 2.1, Option 1

Author: Egil Andresen
Date: August 20, 2003

Table of contents:

0. Abstract

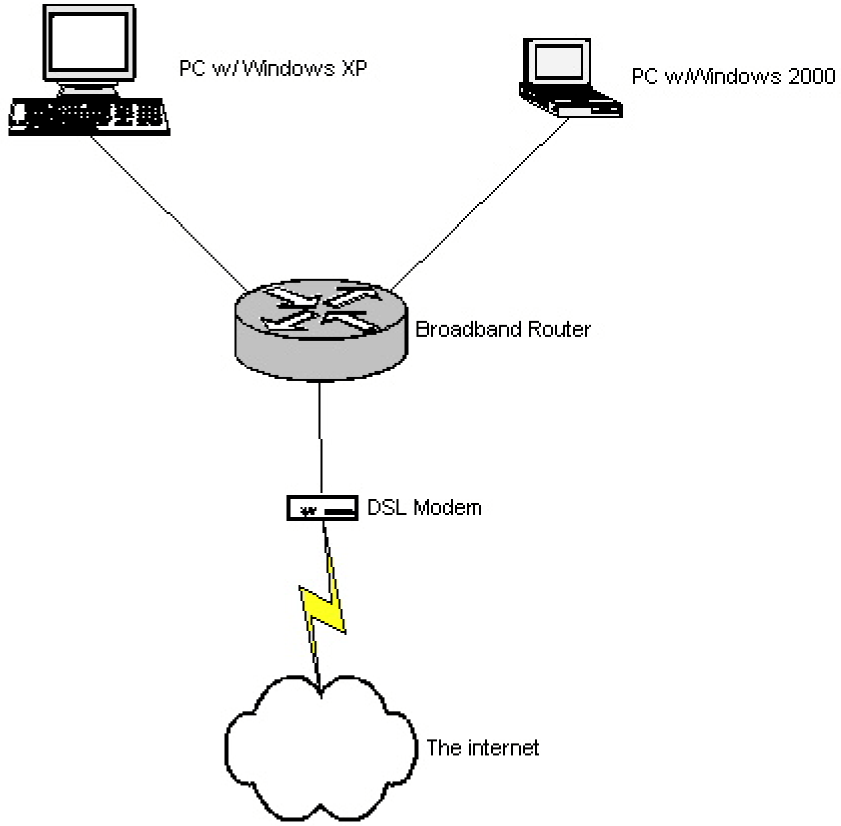
The audit described in this paper will be conducted from the point of view of an administrator and owner of the system being audited. The focus of the audit is on the perimeter defenses in a home office environment. The perimeter defenses are made up of a broadband router (D-Link 604 Ethernet Broadband Router) and personal firewalls running on the computers in the LAN (Kerio Personal Firewall). The audit scope is limited to the technical controls of the perimeter defenses, and do not include organizational or procedural controls. This paper includes a description of the system being audited, an evaluation of risks to the system, an audit checklist, results from the audit of this system, and a discussion of these results.

1. Assignment 1 - Research in Audit, Measurement Practice, and Control

1.1. Identify the system to be audited

Description of the system

The figure below illustrates the network that is the focus of this audit:



This is a common configuration in many homes and smaller offices with a DSL connection and more than one computer. A couple of PCs (in the meaning of Personal Computers) are connected together and access the Internet via the Broadband router, which also has a switching capacity.

The subject of the audit is the perimeter defense. The focus will be on two layers that are defined as the perimeter: the router and the personal firewalls running on the PC's.

The router is a D-Link 604 Ethernet Broadband Router. The router performs Network

Address Translation, DHCP and some simple filtering. Firmware at the time of audit was 1.80. Please note that it is a European version of the router. There are many differences between the US and European versions as regards to both hardware and firmware. The functionality is consequently not entirely similar. The version marketed in the US has e.g. more powerful firewall functions than the one audited here, but lack the capacity to use SNMP.

One of the computers behind the router runs Windows XP Home edition (stationary computer), while the other (a laptop) runs Windows 2000 Workstation. The operating systems on both PC's have been adequately patched.

There is installed a personal firewall on both computers. The firewall is Kerio Personal Firewall version 2.1.5. The firewall was previously known as Tiny Personal Firewall. The main principle behind the firewall is stateful inspection. The administrator can further specify conditions for packet filtering in filtering rules. Apart from checking incoming and outgoing packets, the firewall can also detect if permitted packets are sent by authorized applications.

The DSL modem is provided by the ISP and connects to the ISP through Point-to-Point Protocol over Ethernet (PPPoE). The ISP dynamically assigns the IP addresses, with a new address given every time a new connection is initiated.

A proxy application, Proxomitron, is used for web browsing. The role of the proxy is primarily to stop pop-ups and to control the information given away when browsing the web. The use of a proxy is significant because the rules used by the firewall must be adjusted so that the proxy does not create a hole in the firewall. If not adjusted, any malicious application could use the proxy to gain access to the Internet.

Anti-virus software with updated virus definitions is used on both computers. Software with purpose of identifying and eradicating spyware is also updated and run reasonably frequently.

The ISP supplying the ADSL connection hosts email and web pages. There is therefore no need for a web or mail server within the network.

The functions of the computers

The laptop is used strictly for work purposes. Work-related activities are mainly performed using standard office programs and e-mail, as well as web browsing for research purposes. Some specialist programs are also used. Data stored on the computer is sensitive to the successful accomplishment of work related activities.

The stationary computer doubles as a home family computer and as a computer used for work-related activities. As above when used for work-related activities this is mainly performed using standard office programs, e-mail, as well as web browsing. In addition the computer performs the functions that one usually would find in a home computer: web browsing, e-mail, downloading of files from the Internet, some games, instant messaging etc.

The stationary computer is used by various members of our family for work and leisure activities. The laptop is mainly used by the administrator conducting the audit described in this paper.

The use of the stationary computer for both work-related and leisure activities is not ideal when considering security. The reasons for this arrangement are both historical and practical. I believe you will find a similar mix of leisure and work activities is not unusual in home office environments. The use of the computers is not considered in more depth in this audit because the focus here is on perimeter defense.

The scope of the audit

As mentioned above the subject of the audit is the perimeter defense. The focus will be on the two layers that are defined as the perimeter: the router and the firewalls running on the PC's.

The router performing NAT provides a frontline defense against attacks coming in to the network. Most incoming attacks are presumed stopped by the router. However the firewalls on the computers are also set up to stop incoming attacks as a second line of defense.

Trojans and other malware are considered a major risk in this environment. Outbound filtering performed by the firewall is considered the main defense against this risk. Anti-virus programs can provide some protection against such malware, but an evaluation of their function in this environment is not considered a part of this audit.

When conducting the tests described below related to the personal firewall, I have chosen to perform these on the stationary computer. The setups of the two computers are similar, and Kerio Personal Firewall runs on both computers. But with some variation in use and a different operating system, there are some differences that might affect the results of some audit tests. In real life the tests should be run on both computers. That is considered beyond the scope of the audit described in this paper. The stationary computer was chosen as the basis for the tests related to the personal firewall because the use of this computer is considered to give it a higher risk than the laptop. The consequences of a compromise of either computer are considered to be about the same, but the likelihood of a compromise is considered greater for the stationary computer because of the more varied use.

Some controls that are vital to information security in an organization, cannot be relied upon to any extent in a home office environment such as the one this audit is based upon. In particular organizational and procedural controls are difficult to implement in a home environment. For this reason the focus here is on technical controls.

1.2. Evaluate the risk to the system.

In the international standard ISO/IEC 17799:2000 about information security management the term “information security” is defined as the preservation of:

- Confidentiality - Ensuring that information is accessible only to those personnel authorized to have access

- Integrity - safeguarding the accuracy and completeness of information and processing methods

- Availability - Ensuring that authorized users have access to information and associated assets when required

These principles apply to home offices and small businesses just as much as they would to a bigger organization’s network. Below I have tried to apply these principles as a starting point for reviewing risk in this environment.

Threats to computer systems can be divided into physical threats and logical threats. As in a corporate environment physical threats in a home office environment include theft, fire, flood, magnetic pulses, etc. Physical threats are not considered to be relevant to the area discussed here as we are concentrating on perimeter defense. Instead we will concentrate on logical threats. In this case the focus will be on malicious software and direct attacks on the system.

The specific risks related to broadband connectivity must be considered in this risk evaluation. Broadband connectivity has become popularized among the general public the last few years. Unfortunately, the risks associated with a broadband connection are far greater than with a dial-up-connection. The reasons for this is that broadband connections give the possibility to always be online, in addition to increasing the available bandwidth considerably.

Risk evaluations involve evaluating all possibilities of what might happen – the probable and the improbable. In the table below I have listed the risks considered to be the most important for this system. The table is by no means considered to be complete, but should provide an adequate overview of risks that the audit should consider. The audit should consider how the perimeter defenses mitigates the following risks:

What might happen	Likelihood	Consequences / Impact	Risk Level
The computers might be used as intermediaries for other attacks. For an attacker to be able to use the computer in this way malicious code in general would have to be downloaded and executed	High – Based on prevalence of malicious software	Bad – Damaged reputation, extensive time to resolve problems and clean systems, possible liability issues relating to lack of security to prevent participation in attack,	High
		blocking the internet	

What might happen	Likelihood	Consequences / Impact	Risk Level
		connection by creating massive traffic.	
Theft of information (loss of privacy/confidentiality) as a result of malicious software or direct attack on the system	High - Based on known vulnerabilities in the Windows operating system	Very Bad – Possibility of damage to reputation, business information could fall into the hands of competitors, sensitive private information could be used for e.g. identity theft.	High
Important software or information could be destroyed as a result of malicious software or direct attack on the system	High - Based on prevalence of malicious software	Moderate - Provided adequate backup is available (not considered here) information or systems should not be lost permanently, but the attack will result in the unavailability of the system for a period of time. Extensive time to resolve problems and clean systems.	Medium
Information stored on the computer could be changed (loss of integrity) as a result of malicious software or direct attack on the system	High - Based on known vulnerabilities in the Windows operating system	Moderate–Provided adequate backup is available and it is possible to discover the attack early, original information should be retrievable. Extensive time to resolve problems and clean systems, possible damage to reputation, unavailability of data while resolving issues.	High
The computers could be misused to publish porn images, warez or as a hub for hacker forums.	Medium – storage of this sort of information is a known goal for attackers	Moderate – Extensive time to resolve problems and clean systems, considerably lower performance by the systems, as well as blocking the internet connection by creating massive traffic.	Medium
The computers could be misused to spread spam	Medium – it is known that spammers are looking for 3rd party machines to distribute spam.	Moderate – Extensive time to resolve problems and clean systems, damage to reputation, possibility of being blocked out by sites being spammed, blocking internet connection by creating massive traffic.	Medium

What might happen	Likelihood	Consequences / Impact	Risk Level
Computer users utilize the systems for unapproved purposes (e.g. exchange of files thru P2P applications)	Low – Limited number of people have access and physical positioning of computers makes it hard to conceal unapproved use of resources.	Low – Information could be leaked that could put the systems at risk, possible breach of copyright legislation	Low
Denial of service (DOS) attack target the systems being audited	Low – The likeliness of DOS attacks against this sort of systems seems low.	Low – System will be unavailable for duration of attack.	Low

It is not possible to make a precise estimation of the value of the information assets the computers represent. The dollar-value of the assets will not be particular high on this kind of system, but breaches of security could still cause severe problems for the users. Work-related information and sensitive personal information is stored on the computers. A breach of confidentiality could have implications both in relation to reputation as well as a possibility of financial loss. Availability of the systems is very important, as it to some degree would be difficult to perform work tasks without available systems. The financial risk here is the value of the hours when the system is unavailable and work tasks cannot be performed. Loss of important data as a consequence of an attack is also an issue, as this could give a financial loss as a result of fraud or simply because work might have to be done again.

1.3. What is the current state of practice?

To clarify the current state of practice for the perimeter controls included in this paper, it was necessary to do research both related to personal firewalls and to broadband routers. The starting point for the research was searches using Google. Both general searches for keywords such as "personal firewalls" or "router security", and product specific searches for Kerio Personal firewall and D-link routers was conducted. The searches unearthed some useful web sites and links to similar web pages with relevant information.

Familiar sites with security information were also searched for relevant information. A very useful source was of course the SANS reading room and in particular research papers written by previous students for the GSNA certification. Other sites that were searched include www.securityfocus.com, www.cert.org, http://csrc.nist.gov, http://www.isaca.org, http://www.firewallguide.com and http://www.auditnet.org/isaudit.htm

The National Institute of Standards and Technology (NIST) has issued a guide with recommendations for security for telecommuting and broadband communications. Chapter 3 of this publication concerning firewalls has been a very useful source when developing the checklist, and I have used this as a reference for several items in the checklist in assignment 2. NIST has also produced a document with guidelines regarding firewalls and firewall policy.

There exists considerable research on the subject of firewalls, but personal firewalls have received somewhat less attention. Lance Spitzner's papers "Auditing Your Firewall Setup" and "Building Your Firewall Rulebase" provide a very useful introduction to the subject matter. Some SANS students have researched and written papers regarding personal firewalls that also provide a starting point for creating an audit checklist. In particular I would like to mention Horace B. Jones's paper "Administratively Auditing the Security Provided by Norton Personal Firewall 2002" and Nicolas Shevelyov's paper "Auditing Sygate Personal Firewall 4.2".

None of the sources above covers the particular brand of firewall used in the setup being audited here. I have however found that the firewall has an active user community that provides help and guidance on how to attain an adequate security level using Kerio Personal Firewall. The forum for Kerio Personal Firewall on the "DSL Reports" website provides several useful threads, in particular for creating a good rulebase for the firewall, while there also exists a general security FAQ on the website with relevant information on Kerio Personal Firewall. A FAQ for setting up the firewall is also provided on the www.blarp.com website and there is a guide in French available at http://babin.nelly.free.fr/kerio.htm. I would also like to mention that Dave Shackleford in his research for the GSEC certification wrote a paper about securing the SOHO that included a general tutorial of the Tiny Personal Firewall, which the Kerio Personal Firewall was based upon.

While the security of routers in general has received some attention, little research seems to have been done on the role of broadband routers in securing a SOHO environment. This is not surprising as cheap broadband routers with security features have not been available very long. The SCORE project is in the process of creating a checklist for Linksys Broadband Routers, but that particular project had not reached any conclusion when the research for this project was conducted. The work on securing Cisco routers done by the NSA and as a part of the SCORE project is relevant to this research, but one has to take into consideration that these guides were written to suit quite a different environment. From the SANS reading room Earl Charnick has provided a paper on how to get the most security out of a Linksys Cable/DSL Router. Several articles exist on the Internet on Broadband routers in general, but the information is rarely detailed enough to be of interest here. The security FAQ on the "DSL Reports" website provides some information in this category as well.

In addition the manuals that are provided from Kerio Technologies and D-Link for the products that this audit concentrates on, while not very comprehensive, do point to some security risks and give some advice as to how the makers of the products think they could be secured.

I would also like to mention IT Governance Institutes' COBIT as a source. While this publication does not give information at the level of detail needed to conduct this audit, it is a useful source for determining controls objectives. The domain DS5 – Delivery & Support – Ensure Systems Security is particularly relevant to this audit.

A full list of sources utilized is listed under References below.

2. Assignment 2 –Create an Audit Checklist

2.1. Audit checklist – Introduction

It is to be noted that as no written security policy exists, the audit is based on control processes that are presumed to be part of a “best practice”. This complicates the audit, as it is no clear design of a security model and no specific items to check against.

In some cases there are more than one test focusing on the same control objective. The tests would focus on different aspects of the objective.

A lot of tests involve accessing information in the router’s web-based administration interface. In this interface there are tabs on top of the page representing the “main menu”, and further menus on the left depending on your choice in the main menu. Below the pages are referenced as <Main menu choice> - <sub menu choice>. For example “Tools – Misc” means choosing the item “Tools” on top of the web page and then the item “Misc” to the left on the page.

Directory of tests:

1. Router – authentication
2. Router – remote access SNMP
3. Router – remote access web
4. Router – disconnect
5. Router – pingable
6. Router – remote scan
7. Router – firewall
8. Router – services allowed
9. Router – Inbound filter
10. Router – Outbound filter
11. Router – log information
12. Router – log attacks
13. Router – firmware
14. Firewall – startup
15. Firewall – authentication
16. Firewall – remote access
17. Firewall – principles for ruleset
18. Firewall – service rules
19. Firewall – application rules
20. Firewall – leaktest
21. Firewall – stop engine
22. Firewall – port scan
23. Firewall – log
24. Firewall – updates

2.2. Audit checklist – D-Link Broadband router

Test: 1. Router – authentication	Analysis: Objective
Control objective: Only authorized persons should have access to administrative functions for the router**.**	
Risk: An unauthorized insider or a remote attacker could access the router, gain control over it and change all its settings at will. This could put at risk the availability of communication services and the confidentiality of data being communicated, as well as provide a basis for further attacks against the computers behind the router.	
Reference: D-Link, "DI-604 Express Ethernetwork Broadband Router Manual", Rev. 102202, pages 10-11 and 31-32 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., "Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology", pages 9 and 12	
Procedure: Access the router's web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. A window will pop up asking for username and password (default username, which cannot be changed is, "admin"). Try to log on to the router using a blank password. Try to log on to the router using an invalid, randomly chosen password.	
Compliance: It should not be possible to log on to the router without typing a valid password.	
Comments: The default password is blank. A wizard can be run at start up which encourages a change of password, but it is up to the administrator whether or not he actually wants to do this. It is presumed that only authorized users know the password.	

Test: 2. Router – remote access SNMP	Analysis: Objective
Control objective: It should not be possible to access the administrative functions of the router from outside the LAN.	
Risk: Attackers could attain remote access to administrative functions on the router, gain control over it and change all its settings at will. This could put at risk the availability of communications services and the confidentiality of data being communicated, as well as provide a basis for further attacks against the computers behind the router. It might also be possible to steal the User-ID and password used to connect to the ISP and abuse the account.	

Reference:
Arhont Information Security, “Security issues in D-Link DSL-300/DSL-300G+ Broadband Modem/Router”

Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 13

Center for Internet Security, “Benchmark for Cisco IOS – Level 1 and 2 benchmarks – Version 2.0”, rules 3.1.6 – 3.1.10

Procedure:

- Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.
- Check on the web administration pages for the router (page Advanced – SNMP) if the option for remote access to the router using SNMP is activated.
- Access the web page Status – Device Info to find the current public IP address used by the router.
- Download SNScan from www.foundstone.com and install it on a separate computer on the WAN side of router.
- Scan the router from the computer on the WAN side using SNScan. Use the public IP address of the router as identified above. Scan all four ports that the tool allows using community strings “public” and “private”.

Compliance:
The test is passed if the web-based administration interface shows that remote access to SNMP is disabled and SNScan is not able to find any information when scanning the router.

Comments:
When remote access to the router using SNMP is allowed, tests have showed that SNScan are able to identify port 161 as accessible.

“Public” and “private” are the default community strings for the router if SNMP is used. Both are well-known and should be changed if SNMP is needed.

Test: 3. Router – remote access Web	Analysis: Objective

Control objective:
It should not be possible to access the administrative functions of the router from outside the LAN.

Risk:
Attackers could attain remote access to administrative functions on the router, gain control over it and change all its settings at will. This could put at risk the availability of communication services and the confidentiality of data being communicated, as well as provide a basis for further attacks against the computers behind the router

Reference:
D-Link, “DI-604 Express Ethernetwork Broadband Router Manual”, Rev. 102202,

page 31-32 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 13
Procedure: Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. Go to the web page Tools – Admin. Check if the option for remote access to web administration functions is unchecked on the web page
Compliance: The option for remote access to web administration functions should be unchecked in order to disallow remote access to perform administrative tasks on the router.
Comments:

Test: 4. Router – disconnect	Analysis: Subjective
Control objective: The router should only maintain a connection to the Internet when there is an actual need to communicate	
Risk: An “always-on” connection can give an attacker time to analyze the system and identify weaknesses. An attacker can then perform better-targeted attacks, which increases the risk that the router and the computers behind it can be compromised.	
Reference: D-Link, “DI-604 Express Ethernetwork Broadband Router Manual”, Rev. 102202, page 18-19 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 10 and 12	
Procedure: Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. Access the web page Home - WAN. Check the value for the parameter “Maximum idle time”. Access Internet. Let the connection remain inactive for a longer time period than indicated by the specified parameter. Access the web page Status – Logs. Check the log if and when the connection was dropped. Attempt to access the Internet. Check the logs to verify that a new connection has been established with a new IP address.	
Compliance: The parameter “Maximum idle time” should be set at a reasonable value. The router should drop the connection after the specified time of inactivity. When a new connection is established the router should have a different IP address on the	

WAN side.

Comments:

The less time the router is connected to the Internet and the more frequent the external IP-address of the router is changed, the less time an attacker will have to analyze the system. The ISP changes the IP address every time the router initiates a new session. The router can disconnect from the Internet after a specified number of seconds of inactivity. The auditor and administrator should consider what a reasonable value for the parameter is. As this is a subjective question it is no given answer to the question.

There is a trade-off between security and functionality regarding this function. Reconnecting to the Internet means that e.g. a web page that the user requests will take a few seconds longer to load than normal. Obviously the router cannot be set to drop the connection after a very short time of inactivity, as this would make the connection slow and surfing the web would not be a pleasure.

A connection can be initiated automatically by services running on the computer, which can somewhat defeat the purpose of this control. That is not the case in this set-up. The home network being audited offers no external services and the benefits of running services that connect automatically is considered to be smaller than the increased risk that the “always-on”-connection gives.

Test: 5. Router – pingable	Analysis: Objective

Control objective:

Untrusted systems that scan the router should not find any information that could compromise the security of the router and the systems behind it.

Risk:

If untrusted systems can identify the router, this can be a first basis for further reconnaissance and a possible attack against the router. Various attacks using ICMP exists, including DOS attacks.

Reference:

D-Link, “DI-604 Express Ethernetwork Broadband Router Manual”, Rev. 102202, page 35-36

Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, pages 10-12

Procedure:

Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.

To identify the router’s current IP-address, access the web page Status - Device Info.

Access a separate computer from the one being audited with a remote location. Open a command line window. Try to ping the router giving the IP address found above.

Compliance:

Test passes if system being audited does not respond to pings.
Comments: The router can be set to respond to or not to respond to pings from the WAN connection. The parameter determining this can be set by accessing the page Tools – Misc in the administration interface.

Test: 6. Router – remote scan	Analysis: Objective
Control objective: Untrusted systems that scan the router should not find any information that could compromise the security of the router and the systems behind it.	
Risk: If untrusted systems can see or access the router being audited, they can gather information about it and launch attacks based on this information. If ports are found open an attacker can launch specific attacks based on the service presumed using the port.	
Reference: Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, pages 10-12 Spitzner, Lance, “Auditing your Firewall Setup” dethy@synnergy.net, “Examining port scan methods - Analysing Audible Techniques”	
Procedure: Let a computer on the LAN access the Internet. Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. To identify the routers current IP-address, access the web page Status - Device Info. Download and install Nmap on a system separated from the one audited. Connect this system to the Internet Use Nmap from the remote system to scan the router. Command: Nmap -sT -P0 -T 3 xxx.xxx.xxx.xxx (Connect scan, no ping, normal scan speed. xxx.xxx.xxx.xxx is the IP address of the router on the public side)	
Compliance: Test passes if Nmap classifies all ports as filtered.	
Comments:	

Test: 7. Router – firewall	Analysis: Objective
Control objective: The router should only allow connections to be initiated from the LAN. No services on computers in the LAN should be available from the Internet.	
Risk:	

An attacker can make specially crafted packets that individually can seem valid, but which a firewall using stateful inspection techniques could be able to detect. The packets might be used to gain information about the system, launch a DOS attack, or to gain access to its resources.

Reference: Auditor’s experience

Procedure:
To check if the routers functionality as a stateful inspection-firewall (SPI) has been activated:

- Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.
- Access the web page Tools - Misc. Verify if the check box for the parameter SPI Mode has been ticked.

Compliance:

The test is passed if the parameter shows that SPI functionality has been activated.

Comments:
The vendor has not produced any detailed information about this functionality. It is beyond the scope of this audit to analyze exactly how the stateful inspection functionality is implemented, ref. comments under Assignment 3 – Is the system auditable. The item is included in the checklists because it is presumed the functionality improves the security of the router to some degree.

Test: 8. Router – services allowed	Analysis: Objective

Control objective:
The router should only allow connections to be initiated from the LAN. No services on computers in the LAN should be available from the Internet.

Risk:
An attacker could bypass the first line of defense, the router, because of holes created to allow certain services access in to the LAN. Defining virtual servers or putting a computer in the DMZ makes it a lot easier to bypass the router’s protection of the systems behind it. An attacker could then gather information about the systems behind the router, and if any vulnerability was found, try to gain access to the computers. They could then be used to attack others, to store files, or sensitive information could be stolen or destroyed.

Reference:
D-Link, “DI-604 Express Ethernetwork Broadband Router Manual”, Rev. 102202, pages 21-23 and 30

Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 12-13

Procedure:
Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.

Access the web page Advanced – Virtual Server. Verify if any virtual servers have been defined

Access the web page Advanced – DMZ. Verify if a DMZ has been defined in the router.

Compliance:
No virtual servers should be defined on the web page Advanced – Virtual server.

DMZ should be checked as disabled on the web page Advanced – DMZ.

Comments:
The functionality in the router described above is relevant when you are offering services to the Internet community from the computers behind the router. As this is not the case here, these functions should be turned off.

Test: 9. Router – inbound filter	Analysis: Objective

Control objective:
The router should filter inbound connections against illegal values

Risk:
Packets with illogical source IP addresses are invalid and may be an attempted attack against the router or systems behind it. The router or the computers might be compromised if these packets are not blocked. Processing packets from these addresses will also be a waste of system resources.

Reference:
SANS Institute, GIAC System and Network Auditor course book, “Auditing the perimeter”, pages 22-26

Naidu, Krishni, “Firewall checklist”, test no. 9

Procedure:
Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.

Access the webpage Advanced – Filter and check the box for Inbound filter. Check if the filter is enabled and if so which IP ranges that the filter blocks.

Compliance:
The following spoofed, private (RFC 1918) and illegal addresses should be blocked:
Standard unroutables

- 255.255.255.255
- 127.0.0.0

Private (RFC 1918) addresses

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Reserved addresses

- 240.0.0.0

Illegal addresses

- 0.0.0.0

Comments:

Test: 10. Router – outbound filter	Analysis: Objective
Control objective: The router should filter outbound connections against illegal values	
Risk: The local systems can be used to attack or spam other systems with spoofed addresses as a consequence of rogue programs on the systems.	
Reference: Naidu, Krishni, "Firewall checklist", test no. 18	
Procedure: To verify if outbound filters are used, access the page Advanced – Filter and check the box for Outbound Filter. Verify if the filter is enabled and which IP range is given.	
Compliance: The test is passed if the filter is enabled and the IP range given is identical to the one used by the LAN.	
Comments:	

Test: 11. Router – log information	Analysis: Subjective
Control objective: The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.	
Risk: Insufficient logging can break an audit trail and makes it difficult to identify the source for problems/attacks. As a consequence it would be more difficult to remedy problems because of a lack of information about them. More subtle attacks could remain undetected because of a lack of suitable material to identify the attacks.	
Reference: Center for Internet Security, "Benchmark for Cisco IOS – Level 1 and 2 benchmarks – Version 2.0", rule 3.1.49-3.1.54 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., "Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology", page 10-11	
Procedure: Access the router's web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. Access the log page on the router's administration interface (web page Status – Log). In addition access logs that the router has e-mailed to the administrator as specified in the log settings in the administration interface (Status – Log – Log Settings). Inspect the logs. Attempt to find evidence of blocked connections. Review the information given in the logs.	
Compliance:	

The test passes if at least the following information is recorded for each occasion where a connection attempt was blocked:

- Time and date of event (specified at least to the second.)
- Source IP address
- The ports involved
- The protocol used

In addition the information should be on a form that makes it possible to move it to a suitable tool for analysis.

Comments:
The router only keeps a very limited log in its memory and drops all older logged events if it is not instructed to send these on to another system. It is possible to send logs to an e-mail address provided by the administrator or a syslog server. In this test it is presumed that logs are saved by sending them to an e-mail address provided by the administrator.

Test: 12. Router – log attacks	Analysis: Objective

Control objective:
The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.

Risk:
Insufficient logging can break an audit trail and makes it difficult to identify the source for problems/attacks. As a consequence it would be more difficult to remedy problems because of a lack of information about them. More subtle attacks could remain undetected because of a lack of suitable material to identify the attacks.

Reference:
Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 10-11

Procedure:

1. Ref. procedure for test 6 “Router-remote scan” as specified above. Either utilize the results of this test or perform the test again.
2. Attempt to log on to the router with an invalid password, ref. procedure for test 1 Router – authentication.
3. Make note if any of the attempts to scan or attack the router generated alarms on the desktop of the connected computers.
4. Access the router’s web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password.
5. Access the log page on the router’s administration interface (web page Status – Log). In addition access logs that the router has e-mailed to the administrator as specified in the log settings in the administration interface (Status – Log – Log Settings).
6. Inspect the logs to verify if all scans and attacks are adequately logged.

Compliance: The test is passed if the router logs all attempts to scan or connect to it that have been performed with correct specification of the event.
Comments:

Test: 13. Router – firmware	Analysis: Objective
Control objective: The firmware used in the router should be kept adequately up to date.	
Risk: If the firmware is not kept up to date, known vulnerabilities might give attackers an opportunity to compromise the router. If an attacker can gain control over or bypass the router, it is possibly to collect information about and attack the computers on the LAN.	
Reference: Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., "Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology", pages 10 and 12	
Procedure: Access the Internet site of D-Link in Taiwan in order to gain information about released versions of firmware for the router being audited (Link: http://www.dlink.com.tw. Access Technical support > downloads > Broadband > DI 604 (H/W B1)) Access the router's web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. Verify if the latest firmware is used by accessing the web page Tools – Firmware.	
Compliance: The test is passed if the latest firmware as indicated by the supplier is used in the router.	
Comments:	

2.3. Audit checklist – Kerio Personal Firewall

Test: 14. Firewall – startup	Analysis: Objective
Control objective: The firewall should start up automatically when the system is started**.**	
Risk: Use of the system without the protection offered by the firewall leaves the computer without perimeter defenses.	
Reference: Auditor's experience	
Procedure: Start (alt. restart) the computer. When the start-up procedures are finished, check	

that the icon for the firewall is in the system tray. Right-click on the icon and access menu-item Firewall Status to verify that the firewall is running properly.
Compliance: The test is passed if the firewall starts when the computer/Windows starts.
Comments: The administrator can choose whether the firewall should start when the computer is started. This is controlled by a check box “Start Firewall Engine automatically on Windows start-up” under the “miscellaneous” tab in the Firewall administration application.

Test: 15. Firewall – authentication	Analysis: Objective
Control objective: Only authorized users should have access to the firewall administration application.	
Risk: Unauthorized users or scripts run by these may disable the firewall or change the settings**.** This can leave the computer without effective perimeter defenses and an attacker may be able to use its resources, access information or destroy data and programs as he/she pleases. In particular any rogue application that an attacker had been able to place on the computer, would not be stopped if it attempted to establish a connection to the Internet.	
Reference: Broadband reports, Security FAQ, section 2 Kerio Technologies, “Kerio Personal Firewall 2.1 – User’s Guide”, page 8-9 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, pages 11-12	
Procedure: Try to access the firewall administration application (Start > Programs > Kerio Personal Firewall > Firewall Administration). The system should respond with a screen for logging into the system. Attempt to access the administration application for the firewall without giving the correct password.	
Compliance: The test is passed if access to the Firewall administration application is denied when an incorrect password is given	
Comments: The administrator has to choose whether access to the firewall administration application should be protected by a password. This is set by accessing the Authentication tab in the Firewall Administration application, checking the box for “Authentication is required”, and typing in a password in the appropriate field. By default access to the firewall is not password protected. It is in this test presumed that only authorized users know the password that gives access to the administration application.	

Test: 16. Firewall – remote access	Analysis: Objective
Control objective: The firewall administration application should only be accessible from the local system where the firewall is installed.	
Risk: Unauthorized remote users or scripts run by these may disable the firewall or change the settings**.** This can leave the computer without effective perimeter defenses and an attacker may be able to use its resources, access information or destroy data and programs as he/she pleases. In particular any rogue application that an attacker had been able to place on the computer, would not be stopped if it attempted to establish a connection to the Internet.	
Reference: Core Security Technologies, Advisories, “Vulnerabilities in Kerio Personal Firewall” Kerio Technologies, “Kerio Personal Firewall 2.1 – User’s Guide”, page 8 Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology”, page 13	
Procedure: Access the firewall administration application (Start > Programs > Kerio Personal Firewall > Firewall Administration). Click the authentication tab. Check if the “Enable remote administration” box is ticked.	
Compliance: The test is passed if remote administration is not allowed.	
Comments: An exploit concerning the remote access-function in the firewall was discovered in 2003, see reference above. This exploit concerned version 2.14 of the firewall. If the remote access-functionality was not enabled, it was assumed that it was not possible to exploit this bug. A new version (2.15) was issued where this problem had been resolved.	

Test: 17. Firewall – principles for ruleset	Analysis: Subjective
Control objective: The firewall ruleset should be fashioned systematically in accordance with best practice and in a way that supports the security of the system	
Risk: A firewall ruleset not built according to principles of good security will allow more connections to be made than necessary to achieve the functionality that the system is supposed to have. This increases the risk for security exposures that attackers could utilize. If the firewall ruleset has not been build systematically it is much easier for the administrator to make mistakes when editing the rules. As a consequence the rules might not function as intended and security exposures might arise.	
References: Broadband reports, Security FAQ Broadband reports - Forums - Kerio - Tiny Support, “Example IP rules” Broadband reports - Forums - Kerio - Tiny Support, “[Kerio] Generic Rule Set for Kerio (Proxy and no proxy)”	

Broadband reports - Forums - Kerio - Tiny Support, “Just one example of rules”

CrazyM, “Customizing Firewall Rules - Final Block Rules”

CrazyM, “Customizing Firewall Rules - Global Permit/Block Rules”

Blarp, “Kerio Personal Firewall FAQ”

Optimix, “Kerio Personal Firewall”

Spitzner, Lance, “Building Your Firewall Rulebase”

Procedure:
Access the firewall administration application (Start > Programs > Kerio Personal Firewall > Firewall Administration). Click the “Advanced” button on the screen under the “Firewall” tab. Review the rules specified under the “Filter Rules” tab in relation to the terms for compliance specified below.

Compliance:
The general principle of the terms for compliance is that possible connections allowed by the firewall should be the least possible while maintaining needed functionality (ref. principle of least privilege). In practice the test is deemed as passed if the rules specified are in accordance with the following principles:

- There should be a general rule that blocks and logs all connections that are not specifically allowed.
- To ensure availability of suitable information for analysis of possible security events (audit trail), rules that specify to block a connection should in general be logged
- The rules should generally follow a suitable order. This is important because of the order in which the firewall application process the rules. An orderly ruleset also helps to avoid mistakes when updating the rule set. As an example the ruleset could start with LAN rules, followed by general connectivity rules (DNS, DHCP etc), rules for proxy and loopback rules, rules for specific application and finally general blocking rule(s).

Comments:
This test and the two following are very much subjective tests where the auditor’s good judgment is essential.

Test: 18. Firewall – service rules	Analysis: Subjective

Control objective:
Services should only be allowed to connect to the Internet if this is needed to maintain necessary functionality for the users of the computers.

Risk:
If you allow more services than necessary, you increase the risk that malicious software could make outbound connections. It also increases the likelihood that security exposures might be present that an attacker could use to make an inbound connection and compromise the system.

References:
Broadband reports, Security FAQ

Broadband reports - Forums - Kerio - Tiny Support, “Example IP rules”

Broadband reports - Forums - Kerio - Tiny Support, “[Kerio] Generic Rule Set for Kerio (Proxy and no proxy)”

Broadband reports - Forums - Kerio - Tiny Support, “Just one example of rules”

CrazyM, “Customizing Firewall Rules - Global Permit/Block Rules”

CrazyM, “Customizing Firewall Rules - System Wide Rules”

Blarp, “Kerio Personal Firewall FAQ”

Optimix, “Kerio Personal Firewall”

Procedure:
Access the firewall Administration application (Start > Programs > Kerio Personal Firewall > Firewall Administration). Click the “Advanced” button on the screen under the “Firewall” tab. Review the rules specified under the “Filter Rules” tab in relation to the terms for compliance specified below. Also click the “Microsoft Networking” tab and review the entries here if any.

Compliance
The test is passed if the rules specified are in accordance with the following principles:

- LAN rules should allow only the IP addresses, services and ports that are needed to perform normal operations.
- All ICMP services that are not needed should be blocked.
- IGMP (Internet Group Management Protocol) should be blocked if not needed.
- SSDP (Simple Service Discovery Protocol) should be blocked if not needed.
- Access to port 53 (DNS) should be limited to the specific addresses of the DNS servers that are used. Other connections to port 53 should be blocked and logged.
- Inbound access to port 68 (DHCP) should be limited to the broadband router acting as a DHCP server.
- All ports used by the Netbios services should be blocked both as regards to inbound and outbound connections outside the LAN. If the LAN does not need NetBIOS, then it is advantageous to block these services in general as well as turning them off on the systems. These services can of course be blocked by a general block rule, but the specific high risks associated with these services could make it advantageous to block them specifically to make it easier to identify attempts to set up connections on these ports
- Similar services specific to the Windows operating system (here: XP) should also be blocked if not needed. This include port 135 (Epmap), port 445 (Microsoft-DS) and port 5000(UPnP)).

Comments:

Test: 19. Firewall – application rules	Analysis: Subjective
Control objective:	

Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall

Risk:
If you allow unauthorized applications to connect outbound, spyware or any trojan would be able to communicate at will. Sensitive information could be disclosed, and attackers could take control of the system. Lack of control of applications also increases the likelihood that security exposures might be present that an attacker could use to make an inbound connection and compromise the system

References:
Broadband reports, Security FAQ

Broadband reports - Forums - Kerio - Tiny Support, “Example IP rules”

Broadband reports - Forums - Kerio - Tiny Support, “[Kerio] Generic Rule Set for Kerio (Proxy and no proxy)”

Broadband reports - Forums - Kerio - Tiny Support, “Just one example of rules”

CrazyM, “Customizing Firewall Rules - Application Rules”

Blarp, “Kerio Personal Firewall FAQ”

Optimix, “Kerio Personal Firewall”

Procedure:
Access the firewall Administration application (Start > Programs > Kerio Personal Firewall > Firewall Administration). Click the “Advanced” button on the screen under the “Firewall” tab. Review the rules specified under the “Filter Rules” tab in relation to the terms for compliance specified below.

Compliance
The test is passed if the rules specified are in accordance with the following principles:

- In general applications should not be allowed to act as servers for inbound connections, i.e. inbound connections to application should in general not be allowed.
- Applications given access to make outbound connections are limited to a list of approved applications. The following applications have been approved on the computer being audited:
    - Internet Explorer (only thru proxy except for SSL)
    - The Proxomitron (web proxy)
    - Outlook Express
    - Real Audio Player
    - Windows Media Player
    - Windows Messenger (only for exchanging text-based messages)
    - Spybot – Search and destroy (update)
    - AdAware (update)
    - eTrust EZ Anti Virus (update)
    - WS-FTP
- Only specifically approved applications are given access to use the proxy for establishing outbound connections to the Internet. If access to the proxy is not limited, it could act as a tunnel thru the firewall.

- Applications are only given access to the ports they need to use to provide the wanted functionality. They should also be restricted to specific IP address(es) if applicable.

Comments:

Test: 20. Firewall – leaktest	Analysis: Objective

Control objective:

Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall

Risk:

A rogue application that is able to open up an outbound connection can disseminate confidential data, download malware or use the local system to participate in attacks against other systems.

Reference:

Firewall leak Tester http://www.firewallleaktester.fr.st/ (for downloading leaktests, as well as some information about each of them).

URLs for more information about each individual test:

Leaktest: http://grc.com/lt/leaktest.htm

TooLeaky: http://tooleaky.zensoft.com

FireHole: http://keir.net/firehole.html

Yalta: http://www.soft4ever.com/security_test/En/index.htm

pcAudit: http://www.pcinternetpatrol.com/

AWFT: http://www.atelierweb.com/awft/

CopyCat: http://mc.webm.ru/

Procedure:

1. Download the following test applications from the web page http://www.firewallleaktester.fr.st/ and save them in a suitable catalogue: Leaktest, TooLeaky, FireHole, Yalta, pcAudit, AWFT, Thermite and Copycat.
2. Make sure the system has a connection to the Internet
3. For each test specified below check if the firewall responds with a pop-up warning.
4. Rename Leaktest.exe to a file name of an application that is trusted by the firewall, preferably with the right to access remote port 21 (FTP). Run the test by double-clicking on the exe-file. Click the button “Test for Leaks” in the next pop-up box.
5. Run the test again, but this time in ”stealth-mode”. Procedure as above except hold down the shift key when clicking on the button “Test for leaks”.
6. Run the test TooLeaky by double-clicking on the file tooleaky.exe. Click the “yes” -button in the box that pops up.
7. Run the FireHole test by double-clicking on the file firehole.exe. In the box that

pops up choose to use the default IP address. Click on the “Start” button.

8. Unzip the file Yalta.zip to a suitable catalogue. Run the Yalta test by double-clicking on the file yalta.exe. Enter the IP address of the computer to which a message should be sent, preferably a computer where results can be verified. Perform the test five times entering the port numbers 21, 53, 67, 1030 and 5555 and clicking on the “Classical Leak Test” button.
9. Run the pcAudit test by double-clicking on the file pcaudit.exe. In the next window tick the check box for “I agree” and enter a random text in the provided box.
10. Unzip the awft.zip file to a suitable catalogue. Install the AWFT test application by double-clicking on the setup.exe file and following instructions. Run the test application by choosing start > All programs > Atelier web > Atelier Web Firewall Tester. Press the buttons for tests one to six.
11. Run the Thermite test by double-clicking on the file thermite.exe.
12. Run the Copycat test by double-clicking on the copycat.exe file. Choose the appropriate process and enter the associated PID and hit the Enter button. Hit the enter button again to choose to download the text file from the default location.
13. Check the firewall logs and verify that tests that the firewall blocked have been suitably logged.

Compliance:

The test is passed if none of the test applications are able to establish a connection to the Internet. Specifically the compliance criteria for each individual test is as follows:

Leaktest: Application reports that it was unable to connect or the personal firewall reports that application is trying to access the Internet and asks the administrator’s authorization.

TooLeaky: Application reports it was not able to make an outbound connection

Firehole: Application reports it was unable to make an outbound connection and send a message to an external system.

YALTA: The test pass if the YALTA status bar reports an error while sending, or if the personal firewall reports that YALTA is trying to access the Internet and asks the administrator for authorization.

pcAudit: The application reports that “Your computer is well protected”

AWFT: The test application gives scores to the system being tested based on whether it passes the six tests that the test application is based upon. A perfect score of 10/10 would be needed to pass the test.

CopyCat: The firewall passes the test if CopyCat is not able to place a file named “exploited.txt” in the c:/-catalogue.

For the firewall to pass each individual test, it is also necessary that the firewall in each case gives a warning in a pop up-window and logs the attempt to make an outbound connection.

Comments: In this test it is chosen to test the system running several different test applications. The reason for this is that each test application provides a different method for attempting to bypass security applications and make an outbound connection. Furthermore it is possible to download and execute the tests without using a great deal of resources. The return of using resources running several tests and gaining a better understanding of the possibilities of rogue applications making outbound connections, is considered greater than the costs of running multiple tests. It is a question whether one can expect the firewall to stop all of these leaktests. Some of the tests go after weaknesses in applications or ways to make a program launch another program. Stopping such behavior have not traditionally been a job for firewalls, and require a form of application control or maybe sandboxing. Personal firewalls do though seem to be moving in a direction where such features may be included with the programs. The leaktests also illustrate real risks and have a value as such. It should be cautioned that its is possible that running one or more of the leaktests on your PC might create problems for the stability of some programs or processes. Care should be taken when running these test applications.

Test: 21. Firewall – stop engine	Analysis: Objective
Control objective: Only authorized users should be allowed to stop the firewall engine	
Risk: Malware may try to stop the firewall engine. Non-administrative users may knowingly or unknowingly try to stop the firewall. When the firewall is not in use the system is unprotected against outbound attempts to communicate from e.g. trojans, and leave the router as the only protection against inbound attacks.	
Reference: Broadband reports, Security FAQ For information about the Firewar test application: http://www.paoloiorio.it/fw.htm.	
Procedure: Right click on the Kerio Firewall icon in the system tray. Choose the menu item "Exit". The software will ask if you want to stop the firewall. Click "yes". The software will ask for a password. Type an invalid password in the pop-up box. If the firewall engine actually stopped, restart it for the next test. Access the web page http://www.paoloiorio.it/fw.htm. Download the Firewar test application. Double-click on the downloaded file to run the application. To check if the firewall has stopped, try to access the firewall's status window. Try to surf to a random page on the web. Furthermore try to run one of the leaktests from Test 20 that we know the firewall was successful in stopping. Verify if the leaktest is now able to make a connection to the Internet.	
Compliance:	

The firewall should refuse to stop its engine when an invalid password is given.

The firewall application should not allow other programs to stop its engine. If the firewall engine stops, all traffic to and from the protected machine should be blocked.

Comments:
The Firewar test application may be considered malware by some anti-virus or anti-trojan software. As it might shut down your firewall, this might be understandable. As long as you are aware of its effect and how to restart the firewall engine, it should be safe to run the application. It is though important to use the tool with caution.

Test: 22. Firewall – port scan	Analysis: Objective

Control objective:
Untrusted systems that scan the computers should not find any information that could compromise the security of these systems.

Risk:
If untrusted systems can see or access the system being audited, they can gather information about it, launch attacks based on this information and might be able to compromise the system.

Reference:
Spitzner, Lance, "Auditing your Firewall Setup

dethy@synnergy.net, "Examining port scan methods - Analysing Audible Techniques"

Procedure:
For this test we assume that an attacker has been able to breach the security measures implemented in the broadband router and has full administrative control over it. To gain access to the computers behind the router one possible option for an attacker could be to define a DMZ on the router and put one of the computers in this zone. This would leave the computer completely exposed to the Internet.

We will firstly simulate an attack by defining the stationary computer in a DMZ and port scan the computer from the Internet. Secondly we will disconnect the router, connect the stationary computer directly to the ADSL modem, and do a port scan from the Internet.

Step-by-step procedure:

Access the router's web-based administrative pages by starting Internet Explorer and typing the IP address 192.168.0.1 in the address bar. Type in the correct user name and password. Access the web page Status – Device Info to identify the IP address on the router's WAN side.

Find the computer's IP address in the LAN by opening a command window and typing the command "ipconfig". To define the computer in a DMZ, access the web page Advanced – DMZ in the router's administration interface. Enter the LAN IP address and enable the change.

Download and install Nmap on a system separated from the one being audited. Connect this system to the Internet. Run Nmap using the following command:

```
Nmap -sT -P0 -T 3 xxx.xxx.xxx.xxx
```

(Connect scan, no ping, normal scan speed. xxx.xxx.xxx.xxx is the IP address of the router on the WAN side)

Disconnect the router temporarily and adjust the settings on the stationary computer so that it can be connected directly to the ADSL modem. Connect to the ISP/Internet. Identify the computer's IP address by opening a command window and typing the command "ipconfig".

Run the same test as above using Nmap from a separate computer connected to the Internet and entering the IP address found above.

Compliance:
The test passes if Nmap classifies all ports as filtered on both tests.

Comments:

Test: 23. Firewall – log	Analysis: Objective

Control objective:
The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.

Risk:
Attacks may not be detected or attacks may be misdiagnosed. An attacker could control our system without our knowledge of this, and could steal confidential information, change information stored on the computer or use it to attack other computers. Lack of information about attacks could also make it more difficult and time-consuming to clean the systems after successful attacks.

Reference:
Kerio Technologies, "Kerio Personal Firewall 2.1 – User's Guide", pages 27-29

Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., "Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology", page 10-11

Procedure:

1. Ref. Procedure for test "Firewall-port scan" (Test no. 22) as specified above. Either utilize the results of this test or perform the test again.
2. Ref. Procedure for "Firewall-leaktests" (Test no. 20) as specified above. Either utilize the results of this test or perform the test again.
3. Attempt to access the firewall administration application (ref. Test 15 – Firewall – authentication). When prompted for a password, give an invalid password.
4. Attempt to stop the firewall engine, but do not give the correct password when prompted. (ref. Procedure given in Test no. 21 – Firewall – stop engine)
5. Access the firewall Status window by right clicking on the firewall's icon in the system tray and choosing the menu item "Firewall Status". Choose the logs menu

and “Firewall log” item. 6. Inspect the logs to check if all attacks where logged appropriately.
Compliance: If all the attacks were logged with correct information, the test passed.
Comments: In this test it is presumed that logging is done to the default file c:/programs/kerio/Personal Firewall\filter.log. It is possible to log to a syslog server, and it is also possible to use the firewall without logging. The logging options are chosen by accessing the Firewall Administration application, clicking the Advanced button, and then the Miscellaneous tab.

Test: 24. Firewall – updates	Analysis: Subjective
Control objective: The software that the firewall comprises of should be kept adequately up to date.	
Risk: Known exploits may exist for the firewall software unless properly patched.	
Reference: Auditor’s experience	
Procedure: Right click on the Kerio Firewall icon in the system tray. Choose the menu item “About”. Make a note of the firewall engine version number. Check the version number against information provided on the web page http://www.kerio.com/kpf_releasehistory.html.	
Compliance: The system passes the test if the latest firewall engine version number found on the web page is the same as the one found when checking the firewall version number on the system. If this is not the case, the fixes in versions of the software later than the one in use have to be considered. The fixes in the newer versions have to be considered as a basis of an assessment of the risks associated with not using the latest version.	
Comments:	

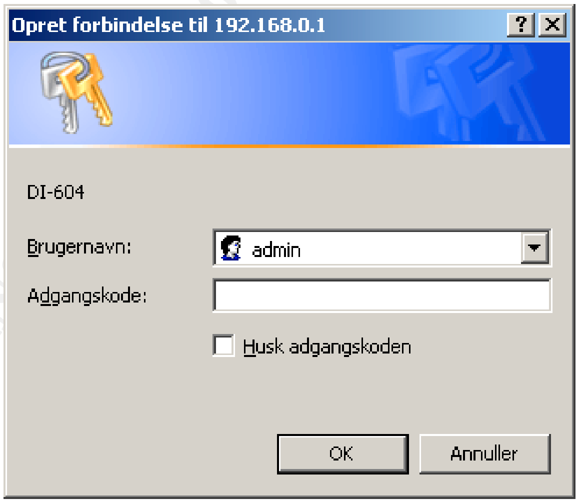
3. Assignment 3 – Audit evidence

3.1. Conduct the audit - Introduction

The following selection of items from the audit checklist reflect the most significant security concerns for the system being audited or support specific findings in the audit:

1. Router – authentication
2. Router – remote access SNMP
4. Router – disconnect
6. Router – remote scan
11. Router – log information
12. Router – log attacks
13. Router – firmware
15. Firewall – authentication
17. Firewall – principles for ruleset
18. Firewall – service rules
19. Firewall – application rules
20. Firewall – leaktest
21. Firewall – stop engine
22. Firewall – port scan
23. Firewall – log

3.2. Conduct the audit – D-Link Broadband Router



Opret forbindelse til 192.168.0.1

DI-604

Brugernavn: admin

Adgangskode:

☐ Husk adgangskoden

Test: 1. Router – authentication
Control objective: Only authorized persons should have access to administrative functions for the router.
Results: When trying to access the router's administration interface an authentication

window above pops up. Trying to log on using a blank password results in the same window popping up again. The use of an invalid password gives the same result. After three attempts with an invalid password, a single word is returned in the browser: "Unauthorized". Renewing the web page gives the possibility to continue to try to log on to the router.

Assessment:

It does not seem to be possible to log on to the router's administration interface without typing in the correct password, which we presume is known only by authorized persons. The router passes the test.

Test: 2. Router – remote access SNMP

Control objective: It should not be possible to access the administrative functions of the router from outside the LAN.

Re

The … er

sho

Acc

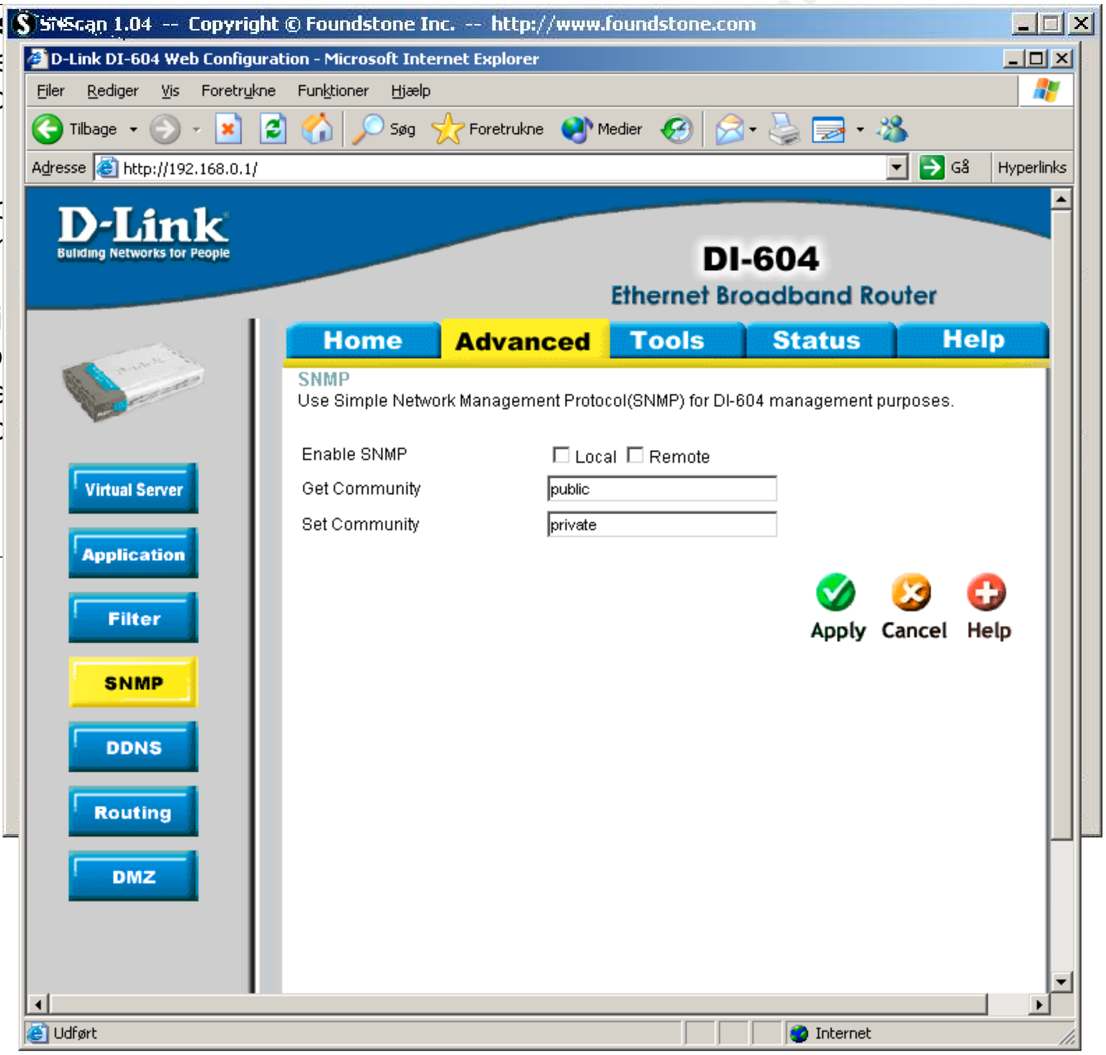
rem

Usi

pro

spe

sup


SNScan 1.04 -- Copyright © Foundstone Inc. -- http://www.foundstone.com
D-Link DI-604 Web Configuration - Microsoft Internet Explorer
Filer Rediger Vis Foretrukne Funktioner Hjælp
Tilbage
Søg
Foretrukne
Medier
Adresse http://192.168.0.1/
Gå
Hyperlinks
D-Link
Building Networks for People
DI-604
Ethernet Broadband Router
Home
Advanced
Tools
Status
Help
Virtual Server
Application
Filter
SNMP
DDNS
Routing
DMZ
Apply
Cancel
Help
Udført
Internet

SNMP

Use Simple Network Management Protocol(SNMP) for DI-604 management purposes.

Enable SNMP ☐ Local ☐ Remote

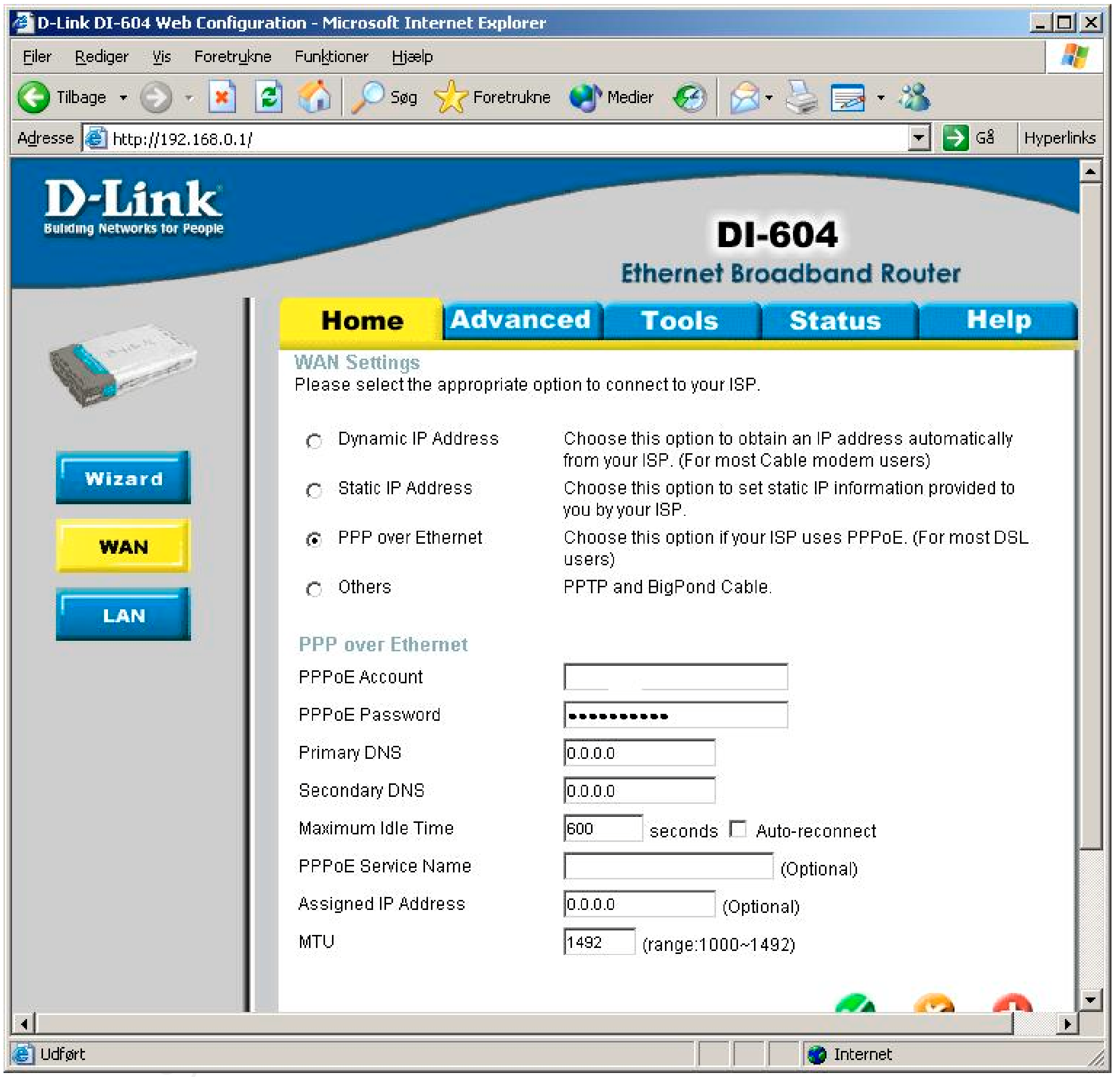
Get Community: public

Set Community: private

Assessment:

The router passes the test. It does not seem to be possible to access the router from a remote location using SNMP.

Test: 4. Router – disconnect



WAN Settings

Please select the appropriate option to connect to your ISP.

○	Dynamic IP Address	Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
○	Static IP Address	Choose this option to set static IP information provided to you by your ISP.
●	PPP over Ethernet	Choose this option if your ISP uses PPPoE. (For most DSL users)
○	Others	PPTP and BigPond Cable.

PPP over Ethernet

PPPoE Account	
PPPoE Password	•••••••••••
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	600 seconds □ Auto-reconnect
PPPoE Service Name	(Optional)
Assigned IP Address	0.0.0.0 (Optional)
MTU	1492 (range:1000~1492)

Control objective: Verify that the connection to the Internet is only active when needed

Results:

The relevant page in the router's administrative interface (Home – WAN) shows the following values:

We notice that the maximum idle time has been set to 600 seconds, i.e. 10 minutes.

Establishing a connection to the ISP and then not make any attempts to establish any connections for the next 10 minutes resulted in the following events as documented by the router log (IP addresses and information that could be identifiable suppressed):

```
Sunday, August 03, 2003 8:44:14 PM PPPoE start to dial-up
*PADI sent
*PADI sent
*PADI sent
*PADO recv 0016 xxxxxxxxxxxx
*PADR sent
*PADR sent
*PADR sent
*PADS recv 8002 D81A
*PAP3: Nextra dialin
*IPCP3: IP is xxx.xxx.xxx.174
*IPCP3: DNS0 is xxx.xxx.xxx.xxx
*IPCP3: DNS1 is xxx.xxx.xxx.xxx
*Syn Time: Sun Aug 03 20:44:36 2003
Sunday, August 03, 2003 8:45:50 PM Unrecognized access from
xxx.xxx.xxx.xxx:1026 to UDP port 137
Sunday, August 03, 2003 8:48:09 PM Unrecognized access from
xxx.xxx.xxx.xxx:1552 to TCP port 445
Sunday, August 03, 2003 8:48:13 PM Unrecognized access from
xxx.xxx.xxx.xxx:1552 to TCP port 445
Sunday, August 03, 2003 8:49:12 PM Unrecognized access from
xxx.xxx.xxx.xxx:4933 to TCP port 445
Sunday, August 03, 2003 8:49:15 PM Unrecognized access from
xxx.xxx.xxx.xxx:4933 to TCP port 445
Sunday, August 03, 2003 8:50:11 PM Unrecognized access from
xxx.xxx.xxx.xxx:1027 to UDP port 137
Sunday, August 03, 2003 8:54:27 PM PPPoE start to hang-up
*PADT sent
*DOD:triggered internally
Sunday, August 03, 2003 8:59:08 PM PPPoE start to dial-up
*PADI sent
*PADO recv 0016 xxxxxxxxxxxx
*PADR sent
*PADS recv 8002 661C
*PAP3: Nextra dialin
*IPCP3: IP is xxx.xxx.xxx.73
*IPCP3: DNS0 is  xxx.xxx.xxx.xxx
*IPCP3: DNS1 is  xxx.xxx.xxx.xxx
```

It can be noted that the router drops the connection after 10 minutes of inactivity. When a new connection is established the ISP has given the router a new IP address.

Assessment:

In my opinion cutting the connection after ten minutes of inactivity is a reasonable timeframe. A shorter period than this could be detrimental to productivity.

The router seems to enforce the rule to cut connection after 10 minutes of inactivity as it is supposed to do, and the ISP changes the IP address when a new connection is made. Minimizing time connected to the Internet and changing IP address frequently makes it difficult for an attacker to gather information about the system and use this to attack it. The system passes the test.

Test: 6. Router – remote scan

Control objective: Untrusted systems that scan the router should not find any information that could compromise the security of the router and the systems behind it.

Results:

Conducting a port scan using nmap as specified in assignment 2 above produced the following results:

```
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-07-31 00:23 CEST
Host xxxxxxxxxx (xxx.xxx.xxx.xxx) appears to be up ... good.
Initiating Connect() Scan against xxxxxxxxxx(xxx.xxx.xxx.xxx) at 00:23
The Connect() Scan took 57 seconds to scan 1643 ports.
Interesting ports on xxxxxxxxx(xxx.xxx.xxx.xxx):
(The 1642 ports scanned but not shown below are in state: filtered)
Port State Service
113/tcp closed auth


Nmap run completed -- 1 IP address (1 host up) scanned in 57.501 seconds
```

The results from the scan show that all ports where filtered except one: port 113, which is sometimes used for identification/authentication.

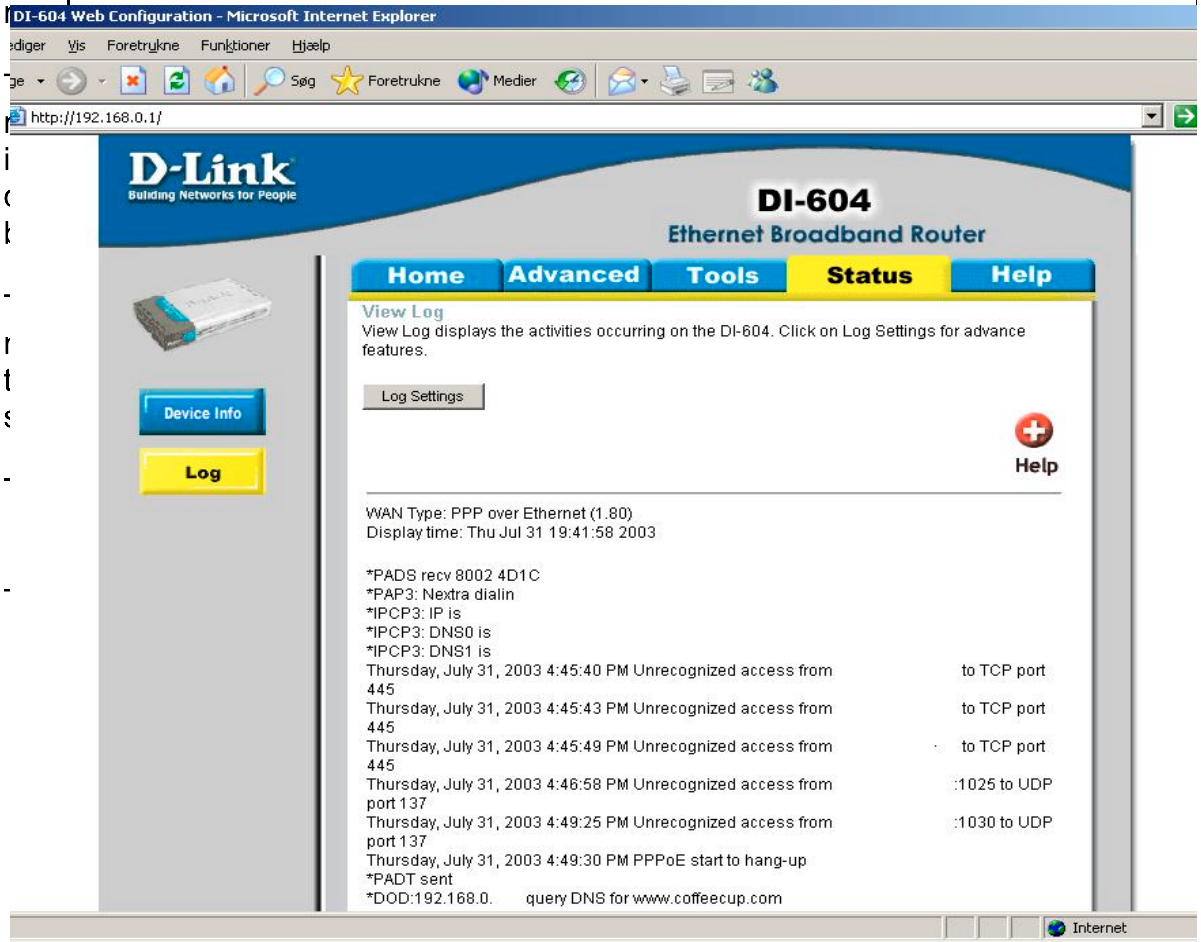
Assessment:
The test was not passed because port 113 was only closed and not stealthed. The risk associated with this finding is not great, but as it serves no purpose having the port unfiltered, the port should be stealthed.

Test: 11. Router – log information

Control objective:
The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.

Results:

Below is a random example of the log displayed in the web-based administration interface for the router. It can be noted that for blocked connections the router logs the time and date, IP address (deleted here to provide security), protocol and port


DI-604 Web Configuration - Microsoft Internet Explorer
Rediger Vis Foretrukne Funktioner Hjælp
Søg Foretrukne Medier
http://192.168.0.1/
D-Link
Building Networks for People
DI-604
Ethernet Broadband Router
Home
Advanced
Tools
Status
Help
Device Info
Log
Log Settings
Help
Internet

View Log

View Log displays the activities occurring on the DI-604. Click on Log Settings for advance features.

```
WAN Type: PPP over Ethernet (1.80)
Display time: Thu Jul 31 19:41:58 2003

*PADS recv 8002 4D1C
*PAP3: Nextra dialin
*IPCP3: IP is
*IPCP3: DNS0 is
*IPCP3: DNS1 is
Thursday, July 31, 2003 4:45:40 PM Unrecognized access from                to TCP port
445
Thursday, July 31, 2003 4:45:43 PM Unrecognized access from                to TCP port
445
Thursday, July 31, 2003 4:45:49 PM Unrecognized access from                to TCP port
445
Thursday, July 31, 2003 4:46:58 PM Unrecognized access from               :1025 to UDP
port 137
Thursday, July 31, 2003 4:49:25 PM Unrecognized access from               :1030 to UDP
port 137
Thursday, July 31, 2003 4:49:30 PM PPPoE start to hang-up
*PADT sent
*DOD:192.168.0.      query DNS for www.coffeecup.com
```

```
Unrecognized access from xxx.xxx.xxx.xxx:1038 to UDP port 137
Unrecognized access from xxx.xxx.xxx.xxx:3616 to TCP port 4662
Unrecognized access from xxx.xxx.xxx.xxx:3616 to TCP port 4662
Unrecognized access from xxx.xxx.xxx.xxx:3616 to TCP port 4662
Unrecognized access from xxx.xxx.xxx.xxx:3616 to TCP port 4662
Unrecognized access from xxx.xxx.xxx.xxx:3472 to TCP port 17300
Unrecognized access from xxx.xxx.xxx.xxx:36733 to TCP port 4662

--- Log End ---
```

Assessment:
The router does not pass the test, as the e-mailed logs do not contain any specification of time for each security event. It is difficult to collect and analyze the log data as the form of the data in the e-mails makes it difficult to transfer them to another tool systematically.

Test: 12. Router – log attacks

Control objective: The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.

Result:

Examples of logs stored in the router and e-mailed to the administrator are given above under test 11.

Port scans and other attacks seem to be logged satisfactorily. All attempts at establishing connections to the router seem to be logged.

When a port scan was performed against the router, this resulted in a stream of e-mails to the administrator. The e-mails were sent as soon as the log was full, and the logs filled up very fast when a port scan was conducted. The administrator should be able to notice brute force attacks quickly thru the sheer volume of e-mails.

Neither successful nor unsuccessful attempts to access the router's administration interface are logged.

Assessment:

The h
the y
e-m

Hov he
test

Tes

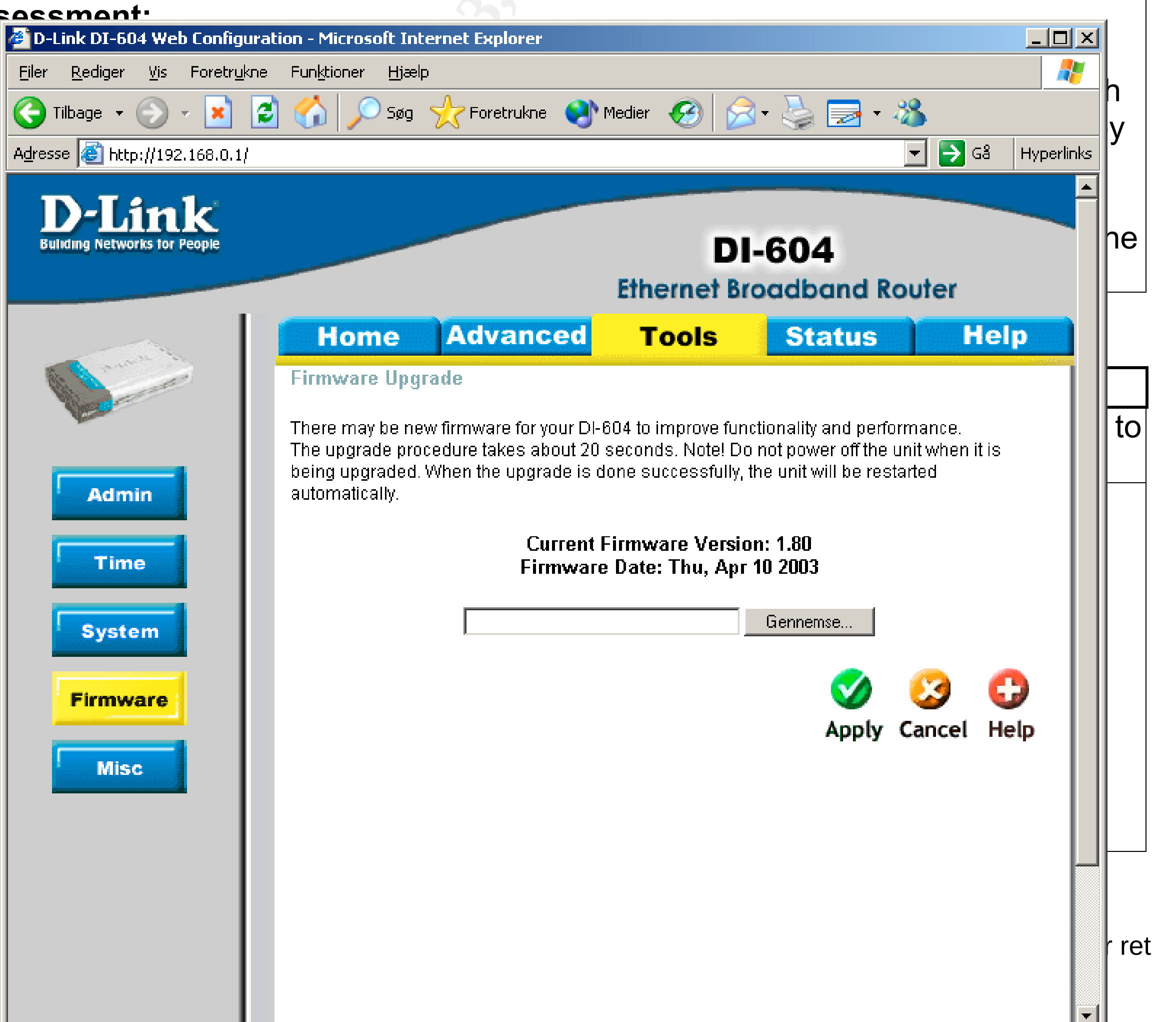
Co to
dat

Re

Fro
rou

Acc
info

As



Firmware Upgrade

There may be new firmware for your DI-604 to improve functionality and performance. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

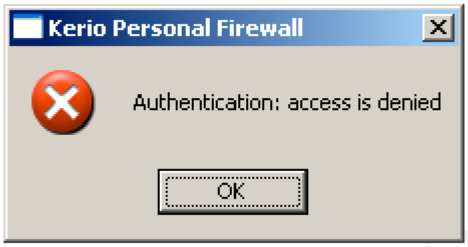
Current Firmware Version: 1.80
Firmware Date: Thu, Apr 10 2003

firmware available for this model.

Assessment:
The router does not pass the test. However D-Link’s information indicate that the only update to the firmware in version 1.81 is to fix some problems relating to the use of UPnP. From a security point of view, using the older firmware is unlikely to have a big effect.

3.3. Conduct the audit – Kerio Personal Firewall

Test: 15. Firewall – authentication	Analysis: Objective


Kerio Personal Firewall

Authentication: access is denied

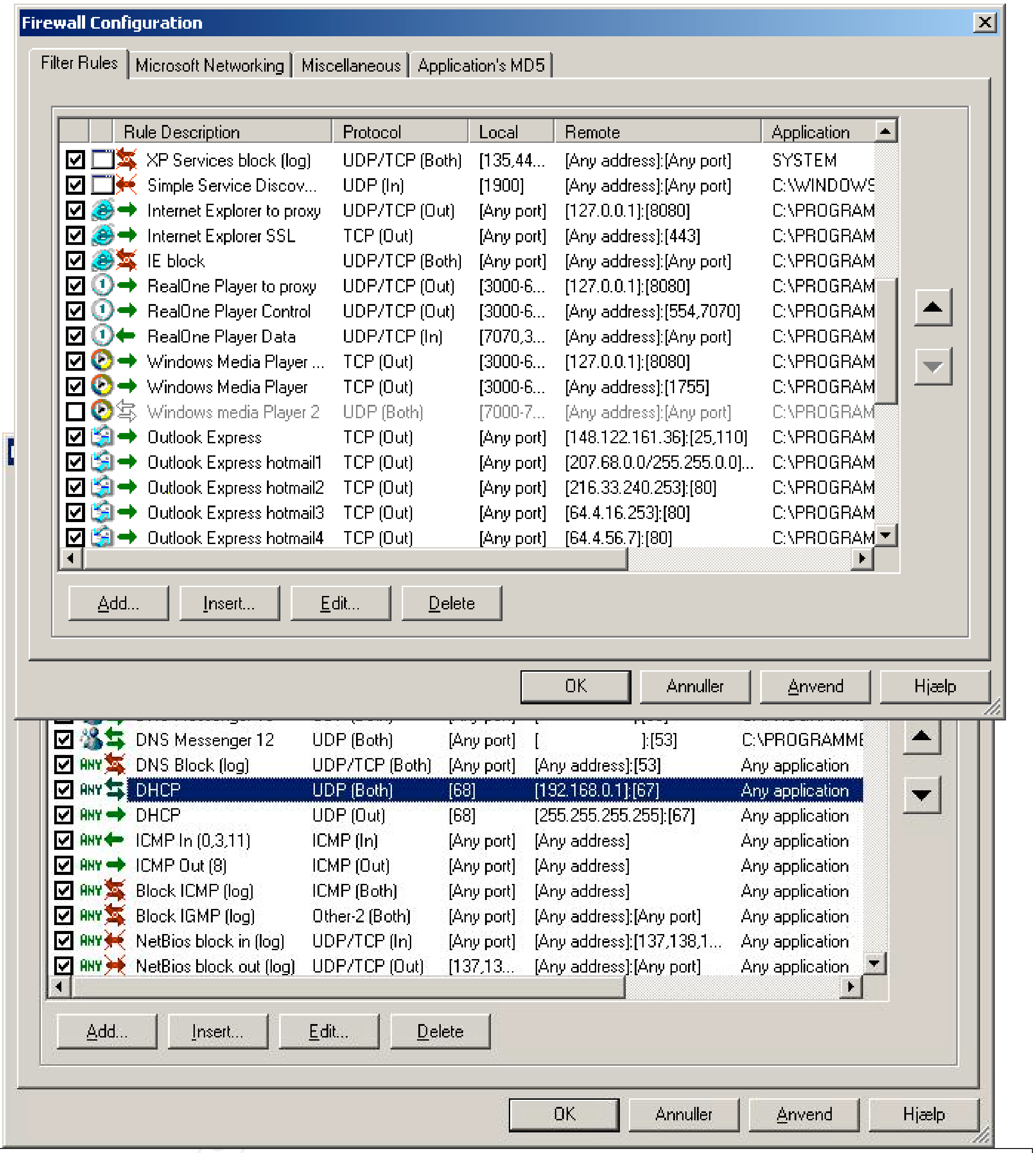
Control objective: Only authorized users should have access to the firewall administration application

Result:
When trying to access the firewall Administration application, the system responds with a screen where you are asked for a password (no username).
If the application is not given the correct password, the following message pops up:

It does not seem possible to access the firewall administration application without knowledge of the correct password.

Assessment:
The system passed the test.

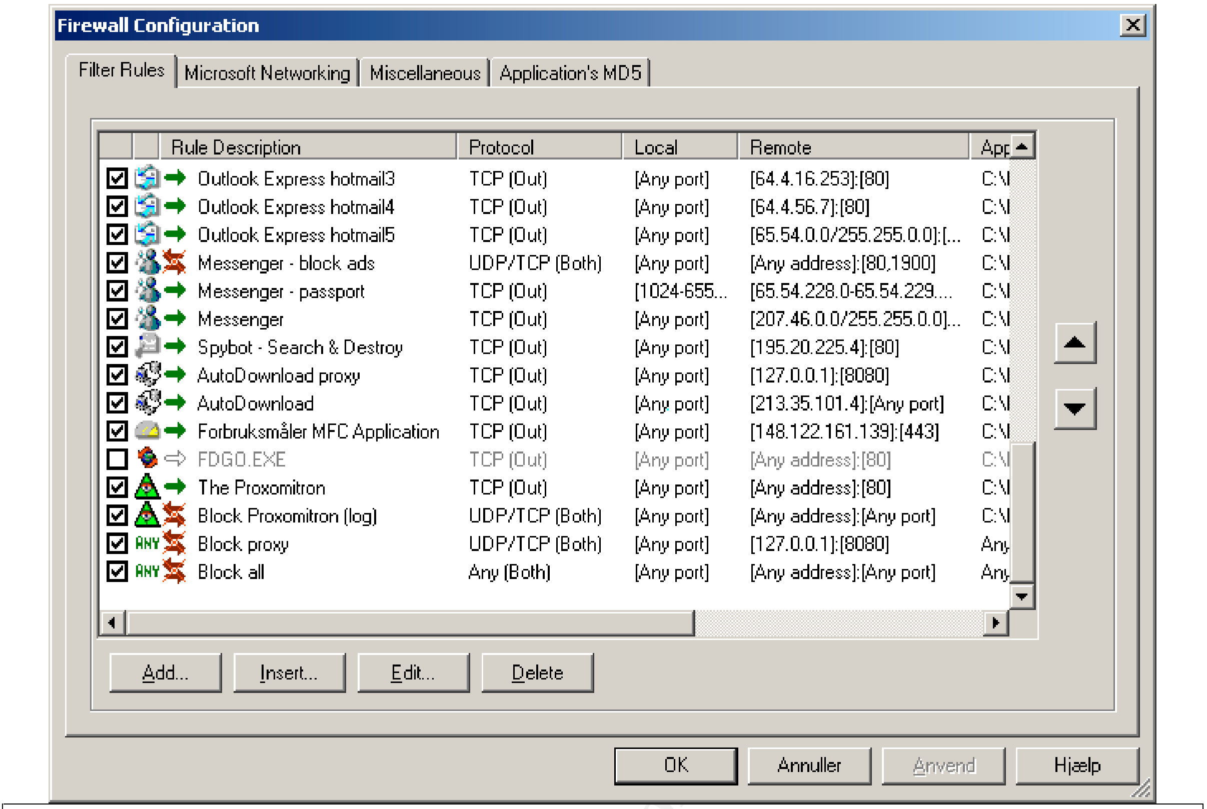
Test: 17. Firewall – principles for ruleset
Control objective: The firewall ruleset should be fashioned systematically in accordance with best practice and in a way that supports the security of the system
Results:



		Rule Description	Protocol	Local	Remote	Application
☑	✗	XP Services block (log)	UDP/TCP (Both)	[135,44...	[Any address]:[Any port]	SYSTEM
☑	✗	Simple Service Discov...	UDP (In)	[1900]	[Any address]:[Any port]	C:\WINDOWS
☑	→	Internet Explorer to proxy	UDP/TCP (Out)	[Any port]	[127.0.0.1]:[8080]	C:\PROGRAM
☑	→	Internet Explorer SSL	TCP (Out)	[Any port]	[Any address]:[443]	C:\PROGRAM
☑	✗	IE block	UDP/TCP (Both)	[Any port]	[Any address]:[Any port]	C:\PROGRAM
☑	→	RealOne Player to proxy	UDP/TCP (Out)	[3000-6...	[127.0.0.1]:[8080]	C:\PROGRAM
☑	→	RealOne Player Control	UDP/TCP (Out)	[3000-6...	[Any address]:[554,7070]	C:\PROGRAM
☑	←	RealOne Player Data	UDP/TCP (In)	[7070,3...	[Any address]:[Any port]	C:\PROGRAM
☑	→	Windows Media Player ...	TCP (Out)	[3000-6...	[127.0.0.1]:[8080]	C:\PROGRAM
☑	→	Windows Media Player	TCP (Out)	[3000-6...	[Any address]:[1755]	C:\PROGRAM
☐	⇆	Windows media Player 2	UDP (Both)	[7000-7...	[Any address]:[Any port]	C:\PROGRAM
☑	→	Outlook Express	TCP (Out)	[Any port]	[148.122.161.36]:[25,110]	C:\PROGRAM
☑	→	Outlook Express hotmail1	TCP (Out)	[Any port]	[207.68.0.0/255.255.0.0]...	C:\PROGRAM
☑	→	Outlook Express hotmail2	TCP (Out)	[Any port]	[216.33.240.253]:[80]	C:\PROGRAM
☑	→	Outlook Express hotmail3	TCP (Out)	[Any port]	[64.4.16.253]:[80]	C:\PROGRAM
☑	→	Outlook Express hotmail4	TCP (Out)	[Any port]	[64.4.56.7]:[80]	C:\PROGRAM

		Rule Description	Protocol	Local	Remote	Application
☑	⇆	DNS Messenger 12	UDP (Both)	[Any port]	[ ]:[53]	C:\PROGRAMME
☑	ANY ✗	DNS Block (log)	UDP/TCP (Both)	[Any port]	[Any address]:[53]	Any application
☑	ANY ⇆	DHCP	UDP (Both)	[68]	[192.168.0.1]:[67]	Any application
☑	ANY →	DHCP	UDP (Out)	[68]	[255.255.255.255]:[67]	Any application
☑	ANY ←	ICMP In (0,3,11)	ICMP (In)	[Any port]	[Any address]	Any application
☑	ANY →	ICMP Out (8)	ICMP (Out)	[Any port]	[Any address]	Any application
☑	ANY ✗	Block ICMP (log)	ICMP (Both)	[Any port]	[Any address]	Any application
☑	ANY ✗	Block IGMP (log)	Other-2 (Both)	[Any port]	[Any address]:[Any port]	Any application
☑	ANY ✗	NetBios block in (log)	UDP/TCP (In)	[Any port]	[Any address]:[137,138,1...	Any application
☑	ANY ✗	NetBios block out (log)	UDP/TCP (Out)	[137,13...	[Any address]:[Any port]	Any application

Querying the firewall administration system shows that the following rules are used (the screenshots give an overview of the rules used and their function. Screenshots detailing each rule is not included here):



		Rule Description	Protocol	Local	Remote	App
☑		Outlook Express hotmail3	TCP (Out)	[Any port]	[64.4.16.253]:[80]	C:\I
☑		Outlook Express hotmail4	TCP (Out)	[Any port]	[64.4.56.7]:[80]	C:\I
☑		Outlook Express hotmail5	TCP (Out)	[Any port]	[65.54.0.0/255.255.0.0]:[...	C:\I
☑		Messenger - block ads	UDP/TCP (Both)	[Any port]	[Any address]:[80,1900]	C:\I
☑		Messenger - passport	TCP (Out)	[1024-655...	[65.54.228.0-65.54.229....	C:\I
☑		Messenger	TCP (Out)	[Any port]	[207.46.0.0/255.255.0.0]...	C:\I
☑		Spybot - Search & Destroy	TCP (Out)	[Any port]	[195.20.225.4]:[80]	C:\I
☑		AutoDownload proxy	TCP (Out)	[Any port]	[127.0.0.1]:[8080]	C:\I
☑		AutoDownload	TCP (Out)	[Any port]	[213.35.101.4]:[Any port]	C:\I
☑		Forbruksmåler MFC Application	TCP (Out)	[Any port]	[148.122.161.139]:[443]	C:\I
☐		FDGO.EXE	TCP (Out)	[Any port]	[Any address]:[80]	C:\I
☑		The Proxomitron	TCP (Out)	[Any port]	[Any address]:[80]	C:\I
☑		Block Proxomitron (log)	UDP/TCP (Both)	[Any port]	[Any address]:[Any port]	C:\I
☑	ANY	Block proxy	UDP/TCP (Both)	[Any port]	[127.0.0.1]:[8080]	Any
☑	ANY	Block all	Any (Both)	[Any port]	[Any address]:[Any port]	Any

Result compared to compliance criteria:

- There is a general block rule as the last rule of the set.
- Detailed study of all the block rules show that all of them are specified to log all instances when the rule is applied. However the naming of rules are not consequent – some specify that logging is done, other block rules do not.
- The ruleset follows a general order, starting with a LAN rule, then loopback rules, general connectivity rules, application rules and finally the rules to block and log all unknown traffic. The order is in my opinion reasonable, even though not strictly in line with the example given in the checklist. Analysis of the rules have not revealed any clear holes in the setup.

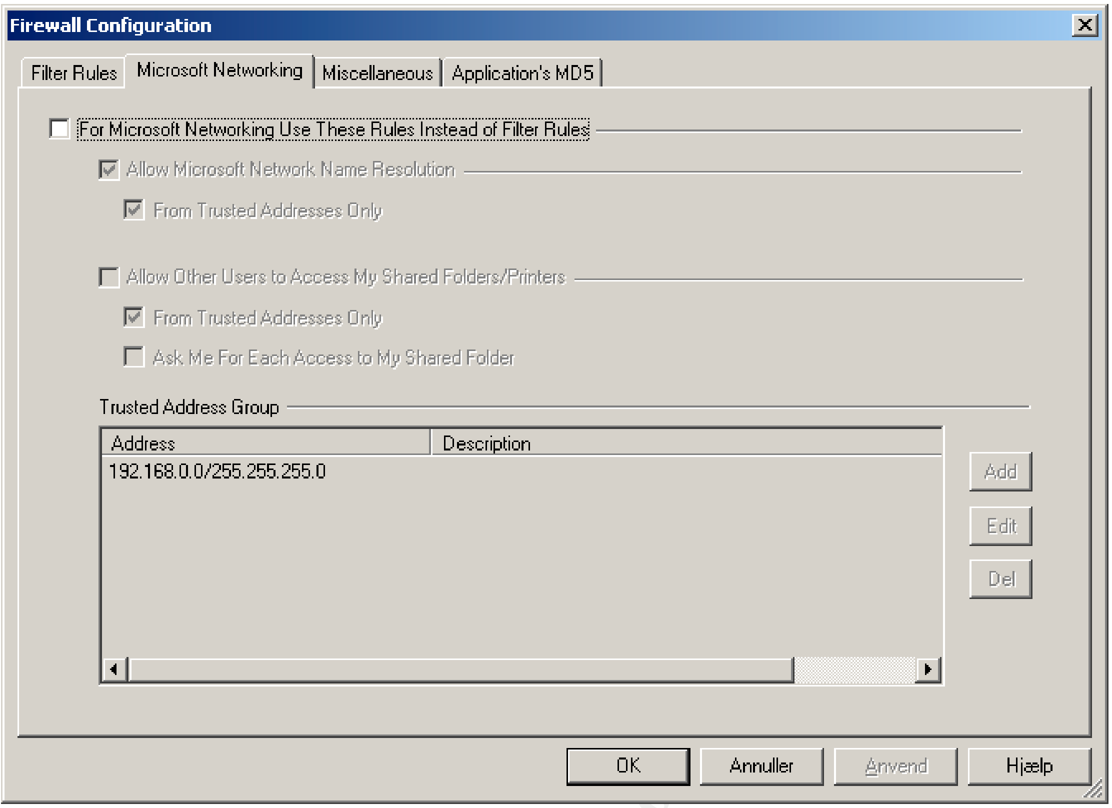
Assessment:

The firewall rules are generally in accordance with the principles for compliance specified above. The rules seem reasonably satisfactory, and the test is considered passed. This does not mean the rules are perfect, they can be improved, but they seem adequate in relation to the principles for compliance.

Test: 18. Firewall – service rules

Control objective:

Services should only be allowed to connect to the Internet if this is needed to



☐ For Microsoft Networking Use These Rules Instead of Filter Rules

☑ Allow Microsoft Network Name Resolution

☑ From Trusted Addresses Only

☐ Allow Other Users to Access My Shared Folders/Printers

☑ From Trusted Addresses Only

☐ Ask Me For Each Access to My Shared Folder

Trusted Address Group

Address	Description
192.168.0.0/255.255.255.0	

maintain necessary functionality for the users of the computers.

Results:

Please ref. test 17 for screenshots documenting the ruleset. The possibility to use special rules for LAN/Netbios under the “Microsoft Networking” tab has not been used for this network as this screenshot shows:

Compared to the compliance criteria, the screenshots show the following:

- The LAN rule allows all traffic to and from computers connected to the local net. Even though the local net is of a minimal size, this rule breaks the principle of limiting access to specific services needed in normal operations.
- The only ICMP services allowed are connected to pinging other machines and performing tracert from the machine being tested. I cannot see any major risk allowing these services, which can be of use to the administrator.
- IGMP and SSDP are both blocked.
- DNS access is limited to the specific servers used by the ISP and the programs that need to access these servers.
- Inbound DHCP is limited to the broadband router.
- Ports used by Netbios and other Windows XP services are blocked in specific rules for all connections outside the LAN.

Assessment:

The LAN rule is more open than specified in the compliance criteria, and for this reason the system fails the test. The rules for the services seem otherwise to be in compliance with the criteria.

Test: 19. Firewall – application rules

Control objective:
Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall

Results:
Please ref. test 17 for screenshots documenting the ruleset. Compared to the compliance criteria, the screenshots show the following:

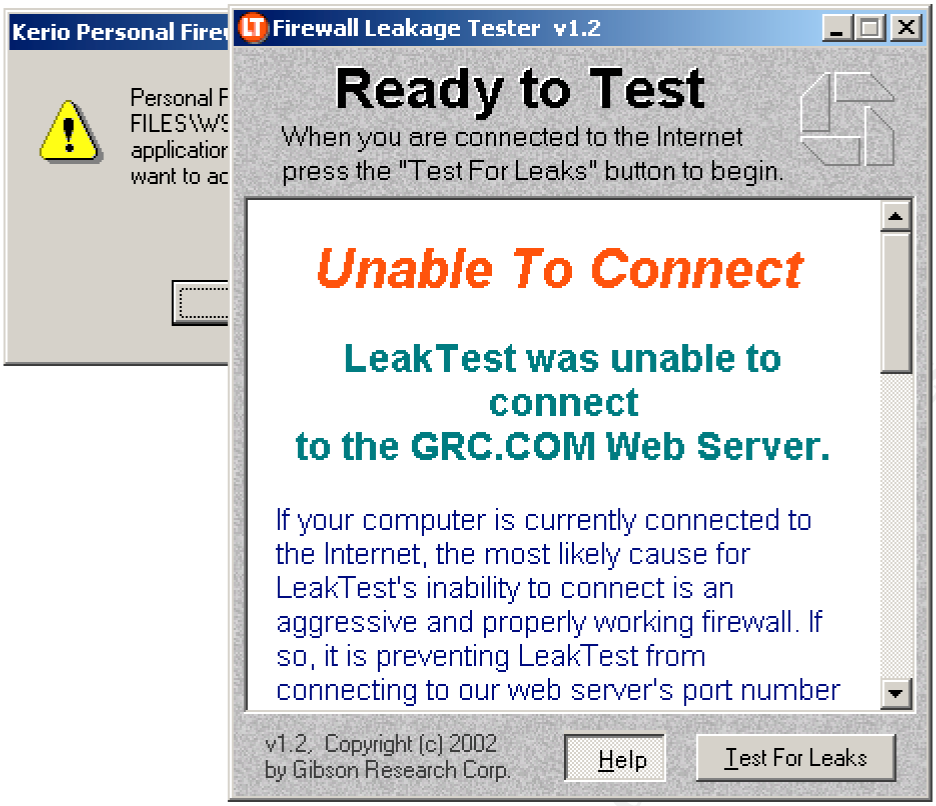
- Applications are in general not given server rights. The only application that accepts inbound connections is RealPlayer. While this may be necessary for the application to perform certain tasks, it can be questioned if the services that need inbound connections are used often, if other temporary solutions can be found if the service is rarely used, and if the gain exceeds the added risks.
- The applications that are given access to the Internet are in accordance with the list above with one exception: a program for measuring Internet traffic has been given access in addition to the ones listed.
- Access to the proxy for Internet access is limited to Internet Explorer, Real Player, Windows Media Player and the application for downloading updates to eTrust EZ Anti-virus. The loopback rules and block rules ensure other applications cannot use the proxy to access the Internet.
- In general applications have only been given permission to access the specific ports that they need. Outlook Express have been limited to access specific IP addresses for the ISPs mailserver and servers connected to the Hotmail service. Messenger is limited to certain IP addresses, though as with Hotmail it has not been possible to limit the addresses perfectly as Microsoft use several servers for the services. Messenger is limited to accessing Microsoft servers and the rules do not permit the application to access other users machines. Update services are limited to specified servers.

Assessment:
The ruleset seem to be in general compliance with the criteria, with the exception that one application (RealPlayer) has been set to accept inbound connections. I addition one application is allowed to make outbound connections, but is not listed in the criteria. There does not seem to be any particular risk connected to this application, but this lapse illustrates the problem of maintaining rules in a changing environment. The test was not passed.

Test: 20. Firewall-leaktest

Control objective:
Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall

Results:



Ready to Test

When you are connected to the Internet press the "Test For Leaks" button to begin.

Unable To Connect

LeakTest was unable to connect to the GRC.COM Web Server.

If your computer is currently connected to the Internet, the most likely cause for LeakTest's inability to connect is an aggressive and properly working firewall. If so, it is preventing LeakTest from connecting to our web server's port number

v1.2, Copyright (c) 2002 by Gibson Research Corp.

Leaktest (procedure points 4 and 5):
When running this test the leaktest program was renamed to WS_FTP95.exe, an FTP client program that was authorized to make connections by the firewall.
Running the test returned the following results:
The firewall warns that the program file has been changed and asks whether the user wants to accept this. An alert user, who knows that no new programs have been installed, should answer “No” (default answer is “Yes” though). Answering “No” to this question returns the following result from the leaktest program:

Running the test in stealth mode returned the same result. A pop-up box warned about the attempts as illustrated. The system passed this test.

TooLea

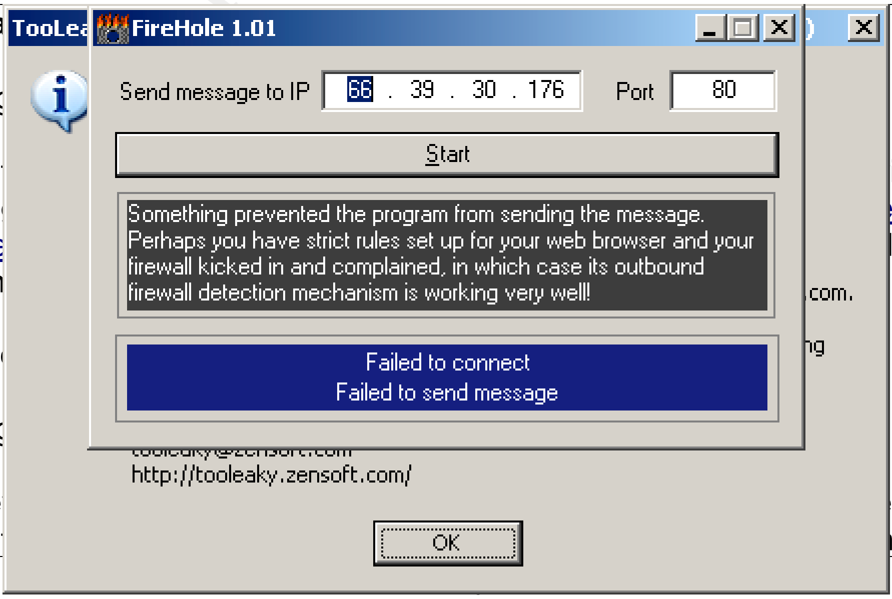
Running

The tes ... ith the following ... rsonal- InfoGoe ... . The firewall failed th

Firehol

Running

The fire ... cause of the rule tha ... ru



Send message to IP 66 . 39 . 30 . 176 Port 80

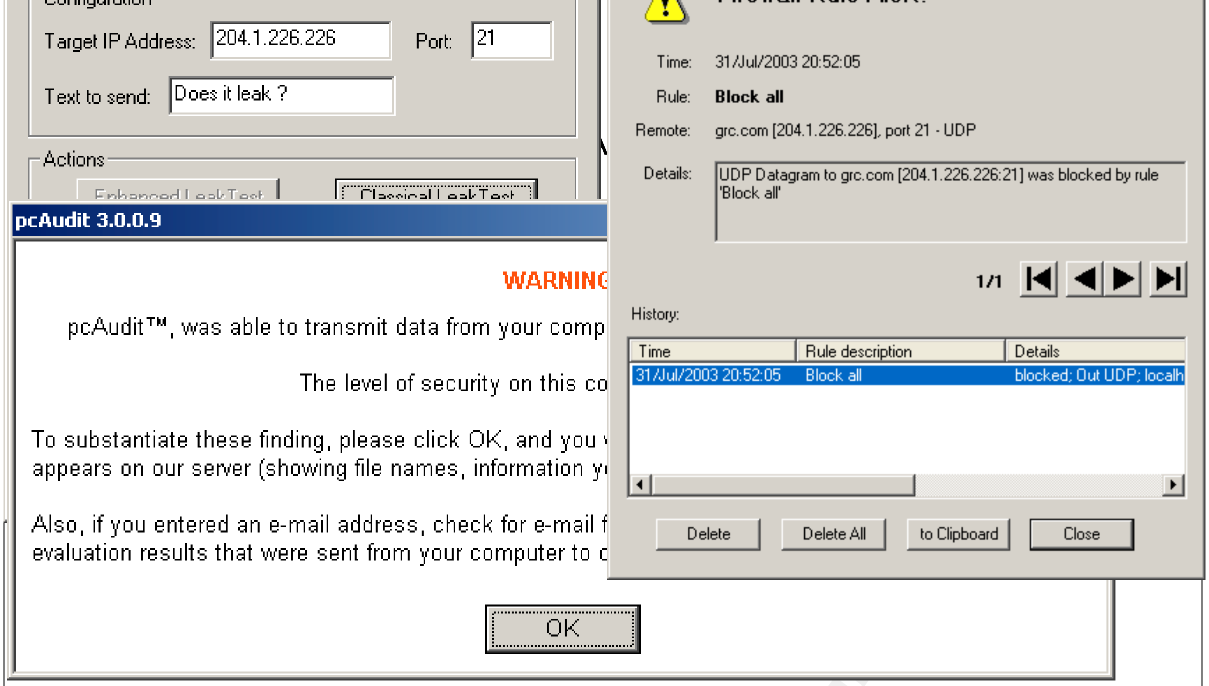
Something prevented the program from sending the message. Perhaps you have strict rules set up for your web browser and your firewall kicked in and complained, in which case its outbound firewall detection mechanism is working very well!

Failed to connect
Failed to send message

.com.

ng

tooleaky@zensoft.com
http://tooleaky.zensoft.com/



Configuration

Target IP Address: 204.1.226.226 Port: 21

Text to send: Does it leak ?

Actions

pcAudit 3.0.0.9

WARNING

pcAudit™, was able to transmit data from your comp

The level of security on this co

To substantiate these finding, please click OK, and you v
appears on our server (showing file names, information yo

Also, if you entered an e-mail address, check for e-mail f
evaluation results that were sent from your computer to c

Time: 31/Jul/2003 20:52:05

Rule: **Block all**

Remote: grc.com [204.1.226.226], port 21 - UDP

Details: UDP Datagram to grc.com [204.1.226.226:21] was blocked by rule 'Block all'

1/1

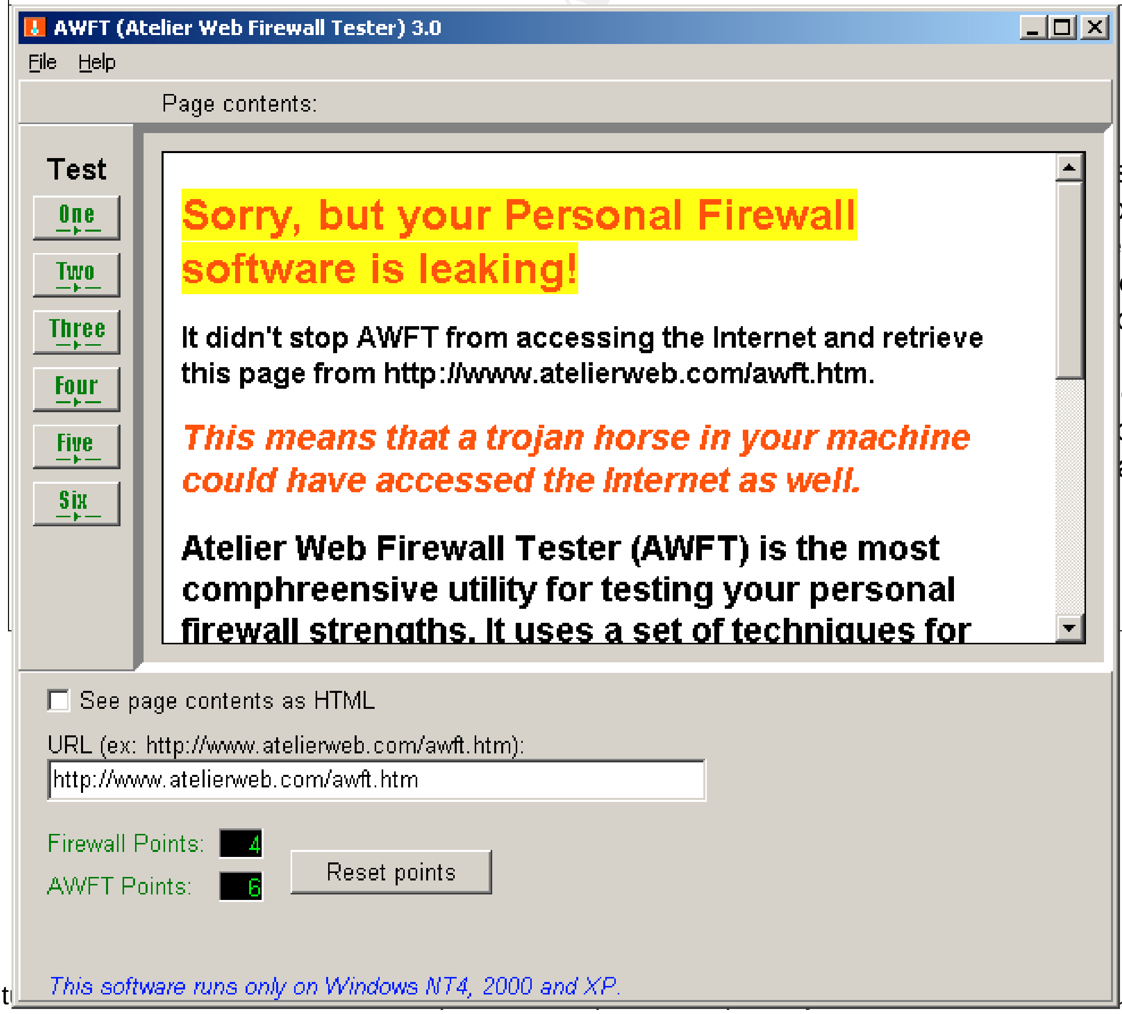
History:

Time	Rule description	Details
31/Jul/2003 20:52:05	Block all	blocked; Out UDP; localh

pcAudit (Procedure point 9)

Running the test returned the following result:

The firewall was unable to stop this test-application, which uses injection of code into a DLL of an authorized application, in accessing the Internet. The system failed the test.



AWFT (Atelier Web Firewall Tester) 3.0

Page contents:

Sorry, but your Personal Firewall software is leaking!

It didn't stop AWFT from accessing the Internet and retrieve this page from http://www.atelierweb.com/awft.htm.

This means that a trojan horse in your machine could have accessed the Internet as well.

Atelier Web Firewall Tester (AWFT) is the most comphreensive utility for testing your personal firewall strengths. It uses a set of techniques for

☐ See page contents as HTML

URL (ex: http://www.atelierweb.com/awft.htm):
http://www.atelierweb.com/awft.htm

Firewall Points: 4

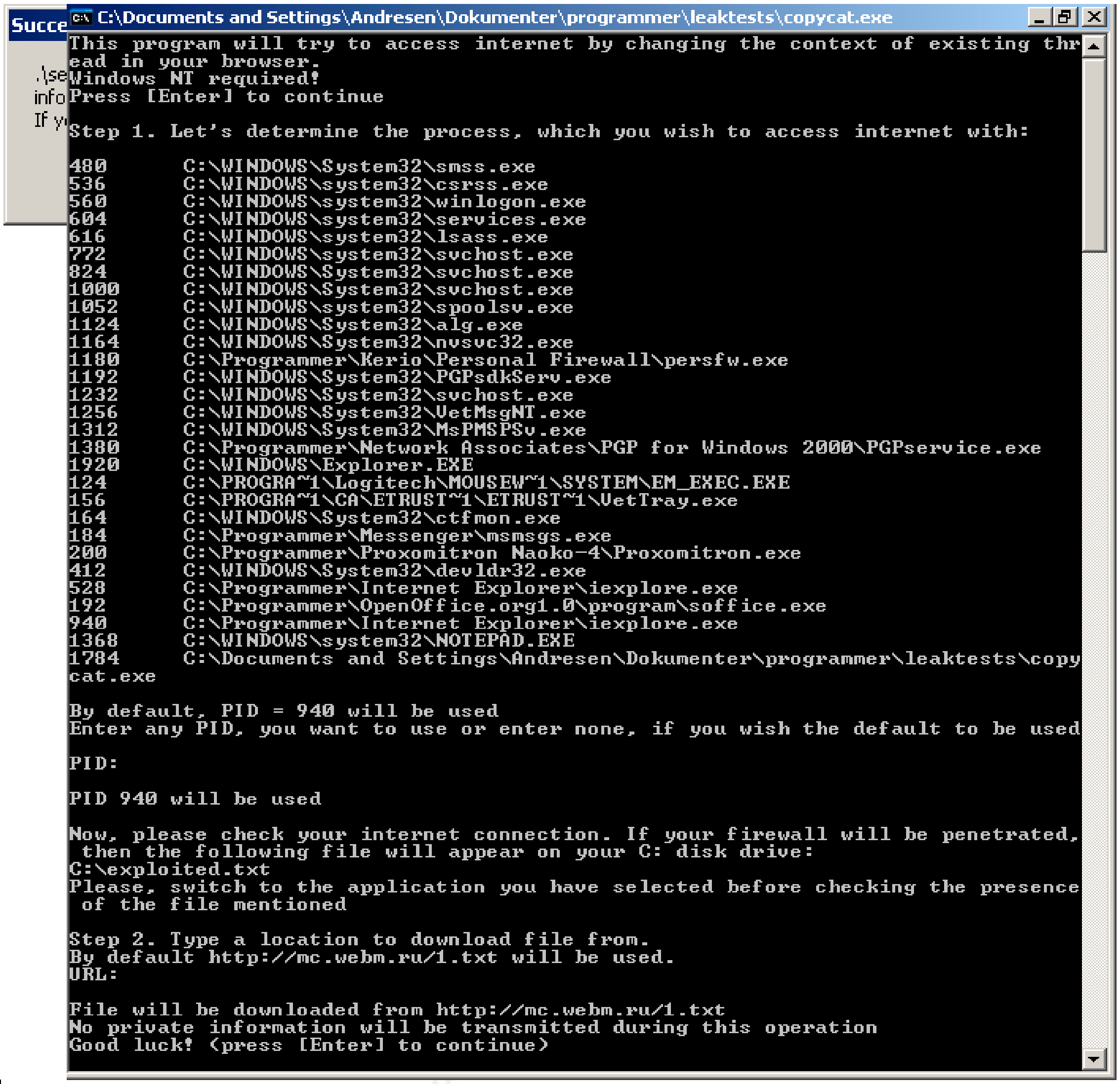
AWFT Points: 6

This software runs only on Windows NT4, 2000 and XP.

ssed
of the
ate a
d a
ory.

o
oes
arned

The


C:\Documents and Settings\Andresen\Dokumenter\programmer\leaktests\copycat.exe
Succe
.\se
info
If y

```
This program will try to access internet by changing the context of existing thr
ead in your browser.
Windows NT required!
Press [Enter] to continue

Step 1. Let's determine the process, which you wish to access internet with:

480       C:\WINDOWS\System32\smss.exe
536       C:\WINDOWS\system32\csrss.exe
560       C:\WINDOWS\system32\winlogon.exe
604       C:\WINDOWS\system32\services.exe
616       C:\WINDOWS\system32\lsass.exe
772       C:\WINDOWS\system32\svchost.exe
824       C:\WINDOWS\System32\svchost.exe
1000      C:\WINDOWS\System32\svchost.exe
1052      C:\WINDOWS\system32\spoolsv.exe
1124      C:\WINDOWS\System32\alg.exe
1164      C:\WINDOWS\System32\nvsvc32.exe
1180      C:\Programmer\Kerio\Personal Firewall\persfw.exe
1192      C:\WINDOWS\System32\PGPsdkServ.exe
1232      C:\WINDOWS\System32\svchost.exe
1256      C:\WINDOWS\System32\VetMsgNT.exe
1312      C:\WINDOWS\System32\MsPMSPSv.exe
1380      C:\Programmer\Network Associates\PGP for Windows 2000\PGPservice.exe
1920      C:\WINDOWS\Explorer.EXE
124       C:\PROGRA~1\Logitech\MOUSEW~1\SYSTEM\EM_EXEC.EXE
156       C:\PROGRA~1\CA\ETRUST~1\ETRUST~1\VetTray.exe
164       C:\WINDOWS\System32\ctfmon.exe
184       C:\Programmer\Messenger\msmsgs.exe
200       C:\Programmer\Proxomitron Naoko-4\Proxomitron.exe
412       C:\WINDOWS\System32\devldr32.exe
528       C:\Programmer\Internet Explorer\iexplore.exe
192       C:\Programmer\OpenOffice.org1.0\program\soffice.exe
940       C:\Programmer\Internet Explorer\iexplore.exe
1368      C:\WINDOWS\system32\NOTEPAD.EXE
1784      C:\Documents and Settings\Andresen\Dokumenter\programmer\leaktests\copy
cat.exe

By default, PID = 940 will be used
Enter any PID, you want to use or enter none, if you wish the default to be used

PID:

PID 940 will be used

Now, please check your internet connection. If your firewall will be penetrated,
 then the following file will appear on your C: disk drive:
C:\exploited.txt
Please, switch to the application you have selected before checking the presence
 of the file mentioned

Step 2. Type a location to download file from.
By default http://mc.webm.ru/1.txt will be used.
URL:

File will be downloaded from http://mc.webm.ru/1.txt
No private information will be transmitted during this operation
Good luck! (press [Enter] to continue)
```

Thermite (procedure point 11)

Running the test returned the following result:

The firewall log shows that the request was detected and denied. The test was not able to make a connection because the firewall does not allow Internet Explorer to connect directly to the Internet ("IE block"-rule). A pop-up box warned about the attempt. The system passed the test.

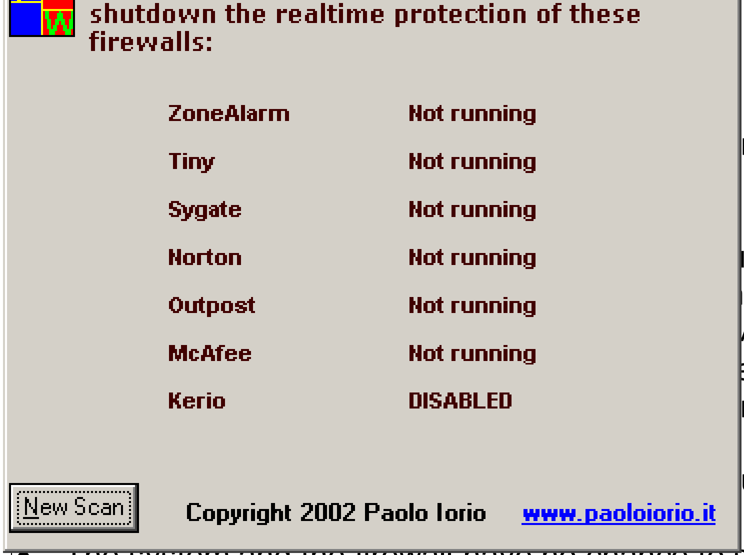
CopyCat (procedure point 12)

Running the test produced the following results:

The test application was able to put a text file downloaded from the Internet on to the computer in the c:/ folder. The application uses process injection to achieve its target. The system failed the test.

Assessment:

The system did not pass all the tests and therefore in principle failed the compliance



shutdown the realtime protection of these firewalls:

ZoneAlarm	Not running
Tiny	Not running
Sygate	Not running
Norton	Not running
Outpost	Not running
McAfee	Not running
Kerio	DISABLED

Copyright 2002 Paolo Iorio www.paoloiorio.it

more. The results of the tests

ıse it can control which
nections and also use MD5
ve not been changed.
e system uses a proxy to
nternet Explorer to initiate
to utilize Internet Explorer to
use of a proxy, the firewall would

- The system and the firewall have no chance to stop the more advanced tests.

The results show that rogue applications that use more advanced techniques would not be stopped by the system when attempting to establish an outbound connection. Fortunately as far as I know, trojans that use techniques such as found in CopyCat are still rarely found in the wild.

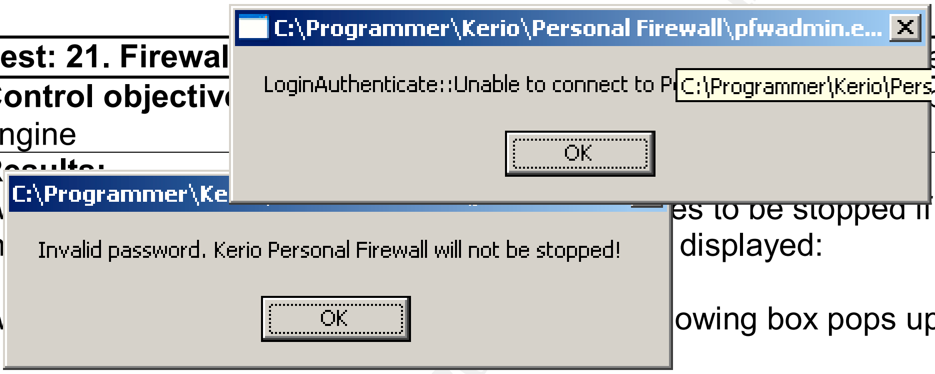
Test: 21. Firewal ective

Control objectiv the firewall engine

Results:

W es to be stopped if it is given an in displayed:

W owing box pops up:



C:\Programmer\Kerio\Personal Firewall\pfwadmin.e...

LoginAuthenticate::Unable to connect to P C:\Programmer\Kerio\Pers

C:\Programmer\Ke

Invalid password. Kerio Personal Firewall will not be stopped!

It appears that the firewall has indeed been disabled, even if the icon still remains in the Windows system tray. When trying to open the firewall's status window, the following error message is received:

The Leaktest (ref. procedure 4 in Test 20) was successfully stopped by the firewall in previous tests. When rerunning this test, the Leaktest application was able to establish a connection to the Internet. It was also possible to surf the web without any restrictions. The system seemingly allowed all traffic to and from the Internet/other systems.

Assessment:
The system passed the test as regards manual stops requiring password. However it failed the test when an application tried and managed to close it down. It appears that the system is vulnerable to malware that might attempt to shut down the firewall application.

Test: 22. Firewall – port scan

Control objective: Untrusted systems that scan the computers should not find any information that could compromise the security of these systems.

Results:

Putting the computer in the DMZ and port scanning from the internet gave the following result:

```
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-08-03 22:54 CEST
Host xxxxxxxx (xxx.xxx.xxx.xxx) appears to be up ... good.
Initiating Connect() Scan xxxxxxxx (xxx.xxx.xxx.xxx) at 22:54
The Connect() Scan took 47 seconds to scan 1643 ports.
Interesting ports on xxxxxxxx (xxx.xxx.xxx.xxx)
(The 1642 ports scanned but not shown below are in state: filtered)
Port State Service
113/tcp closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 47.279 seconds
```

To test further I removed the router and temporarily connected the stationary computer directly to the ADSL modem. Port scanning with this setup gave the following result:

```
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-08-03 23:33 CEST
Host xxxxxxxx (xxx.xxx.xxx.xxx) appears to be up ... good.
Initiating Connect() Scan xxxxxxxx (xxx.xxx.xxx.xxx) at 23:23
The Connect() Scan took 79 seconds to scan 1643 ports.
All 1643 scanned ports on xxxxxxxx (xxx.xxx.xxx.xxx)) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 79.592 seconds
```

Assessment:
When putting the system in the DMZ, the only port that is not classified as filtered is port 113. As seen above (ref. test 7 – router remote scan) it is the router that is responsible for this behavior. This is confirmed when the system is port scanned when it is connected directly to the Internet. Nmap find that all ports are filtered in this test.

The firewall seems to provide an adequate second line of defense. The firewall passed the test.

Test: 23. Firewall – log

Control objective: The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.
Results:

1. Logs from port scans of the computer

The logging capacity was tested when the computer was defined to be in a DMZ and Nmap was used to do a port scan from the WAN side of the router. A pop-up window with warnings immediately appeared as the scan started. The warning is a result of the “Block all”-rule, which blocks all undefined traffic, gives a warning and logs the incident. Below is an excerpt from the log after the port scan:

```
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3051  localhost  2064       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3048  localhost  25         no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3045  localhost  138       SYSTEM
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3042  localhost  135
         C:\WINDOWS\SYSTEM32\SVCHOST.EXE
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3038  localhost  469        no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3035  localhost  120        no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3032  localhost  1548       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3031  localhost  1501       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3029  localhost  1000       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3005  localhost  3001
         C:\WINDOWS\SYSTEM32\ALG.EXE
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3004  localhost  27006      no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3003  localhost  1004       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3002  localhost  1000       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3001  localhost  5801       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  3000  localhost  1501       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  2999  localhost  1548       no  owner
Blocked  Incoming  03/Aug/2003  22:56:35  Block  all   TCP    xxx.xxx.xxx.xxx  2998  localhost  9876       no  owner
```

The information is from left to right: the Rule type (block, permit), direction, date/time, name of rule, protocol, source IP address, source port, destination IP address, destination port and finally name of the local application to which the packet was addressed.

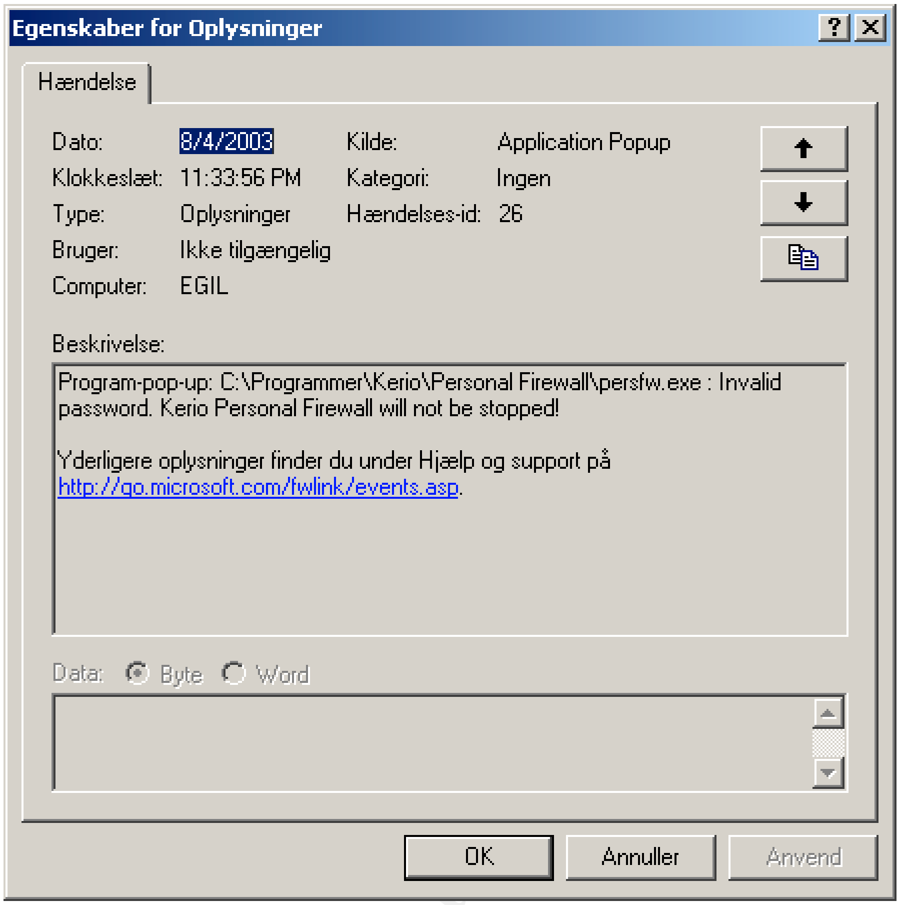
Totally the firewall logged over 2000 incidents as a result of the port scan. Over 99% of the ports scans logged was stopped by the “block all”-rule, but a handful was stopped by other rules (e.g. the DNS block rule for port 53).

2. Logs from leaktests

Those leaktests that the firewall was able to stop, ref. results from test 20, were adequately logged. The logging has the same form as seen above when testing port scans. Windows pop-up when the firewall detects the leaktests, ref. results from test 20.

3. Access firewall administration application, invalid password

If you do not give the correct password when trying to log on to the firewall’s administration application, you will be denied access as documented in test no. 15. However these failed access attempts are not logged by the firewall. As far as I can



Dato: 8/4/2003
Klokkeslæt: 11:33:56 PM
Type: Oplysninger
Bruger: Ikke tilgængelig
Computer: EGIL
Kilde: Application Popup
Kategori: Ingen
Hændelses-id: 26

Beskrivelse:

Program-pop-up: C:\Programmer\Kerio\Personal Firewall\persfw.exe : Invalid password. Kerio Personal Firewall will not be stopped!

Yderligere oplysninger finder du under Hjælp og support på http://go.microsoft.com/fwlink/events.asp.

see they are not logged in the Windows event logs either.

4. *Attempt to stop firewall engine, invalid password*

Kerio Personal Firewall requires a password to stop the firewall engine. Failed attempts to stop the engine because of invalid passwords are not logged by the firewall. However the attempts appear in the Windows log for system events (not in the security log) as an application pop-up window with the following information:

The information in the log is clear when you see the details of the log, but the event looks innocuous when you see it listed in the system event log with a heading of application popup. While this security event is logged, the solution is not ideal.

Assessment:

The firewall keeps logs that give an adequate audit in relation to blocked or suspicious traffic. The firewall passes this part of the test. However there is no logging of successful or failed attempts to access the firewall administration application. The system failed this part of the test.

3.4. Measure Residual Risk

Below is a summary of the results of the tests conducted as a part of this audit. Where the test showed that the system was non-compliant, I have in most cases added a recommendation for a corrective measure.

Test no.	***Title***	***Control objective***	***In compliance***	***Recommendations***
1	Router – authentication	Only authorized persons should have access to administrative functions for the router.	Yes	
2	Router – remote access SNMP	It should not be possible to access the administrative functions of the router from outside the LAN	Yes	
3	Router – remote access Web	It should not be possible to access the administrative functions of the router from outside the LAN.	Yes	
4	Router – disconnect	The router should only maintain a connection to the Internet when there is an actual need to communicate	Yes	
5	Router – pingable	Untrusted systems that scan the router should not find any information that could compromise the security of the router and the systems behind it.	Yes	
6	Router – remote scan	Untrusted systems that scan the router should not find any information that could compromise the security of the router and the systems behind it.	No	Stealth port 113 by forwarding it to an non-existent IP address
7	Router – firewall	The router should only allow connections to be initiated from the LAN. No services on computers in the LAN should be available from the Internet.	Yes	
8	Router – services allowed	The router should only allow connections to be initiated from the LAN. No services on computers in the LAN should be available from the Internet.	Yes	
9	Router – inbound filter	The router should filter inbound connections against illegal values	Yes	
10	Router – outbound filter	The router should filter outbound connections against illegal values	Yes	
11	Router – log	The firewall should provide an	No	Transferring logs

Test no.	***Title***	***Control objective***	***In comp-liance***	***Recommendations***
	information	adequate audit trail and generate alarms when suspicious traffic is detected.		via SNMP to syslog server should be tested
12	Router – log attacks	The firewall should provide an adequate audit trail and generate alarms when suspicious traffic is detected.	No	Acceptable risk/mitigating controls
13	Router – firmware	The firmware used in the router should be kept adequately up to date.	No	Update firmware to 1.81
14	Firewall – startup	Verify that the firewall starts up when the system is started.	Yes	
15	Firewall – authentication	Only authorized users should have access to the firewall administration application	Yes	
16	Firewall – remote access	The firewall administration application should only be accessible from the local system where the firewall is installed.	Yes	
17	Firewall – principles for ruleset	The firewall ruleset should be fashioned systematically in accordance with best practice and in a way that supports the security of the system	Yes	
18	Firewall – service rules	Services should only be allowed to connect to the Internet if this is needed to maintain necessary functionality for the users of the computers.	No	LAN rule should be analyzed and tightened
19	Firewall – application rules	Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall	No	RealPlayer rules should be changed.
20	Firewall – leaktest	Only authorized traffic initiated by authorized applications should be allowed to pass thru the firewall	No	Solutions using other software should be considered
21	Firewall – stop engine	Only authorized users should be allowed to stop the firewall engine	No	Tweak registry keys so that firewall cannot be stopped
22	Firewall – port scan	Untrusted systems that scan the computers should not find any information that could compromise the security of these systems.	Yes	
23	Firewall – log	The firewall should provide an adequate audit trail and generate	No	Acceptable risk/mitigating

Test no.	***Title***	***Control objective***	***In comp-liance***	***Recommendations***
		alarms when suspicious traffic is detected.		controls
24	Firewall – updates	The software that the firewall comprises of should be kept adequately up to date.	Yes	

The audit demonstrated that the system is relatively secure. There are good controls prohibiting access to the LAN from the Internet. The results of the tests indicate that most of the control objectives were met. Almost all the items above where the system wasn't in compliance can be rectified completely or at least mitigated to leave an acceptable risk. The changes that are needed do not require any purchasing cost in most cases, but some man-hours of work from the administrator is needed to make all corrective changes.

Not all changes can be implemented immediately. It is necessary to prioritize the planned system changes. Below I have divided the changes into two groups: changes that can be implemented immediately and changes that require more time to be implemented. The changes in the latter group have been prioritized.

Group 1 – Changes with immediate effect

- Stealth port 113 on router (test 6)
- Update firmware on router (test 13)
- Tighten ruleset for applications in firewall (test 19)
- Tweak registry to stop all traffic when the firewall is disabled (test 21)

While not all of these items represent any great risk, they have in common that they are relatively easy to implement. They do not require additional software or hardware, and do not involve a lot of work. These changes and the results are described in section 4.3 below.

Group 2 – Changes to be implemented over time

1. Stopping rogue applications from making outbound connections (test 20)
2. Tighten rules for the LAN in the firewall ruleset (test 18)
3. Establish system for collecting/analyzing log data from router (test 11)

The list above of areas in need of corrective or mitigating action is in a prioritized order based on the administrator's assessment of the risk that each of the issues represent for this network. More information about possible solutions to mitigate these items are reviewed below.

I have not found any mitigating controls for the lack of logging of successful or unsuccessful attempts to access the router's or firewall's administration interfaces (test 12 and 23). This problem is considered in section 4.4 below

As regards the changes classified in group 2 above, the following suggestions will be considered to mitigate the vulnerabilities:

1. *Stopping rogue applications from making outbound connections (test 20)*

   While the firewall has adequate controls over the usual user applications that would want to establish connections to the Internet, there are not adequate controls built into the system to stop rogue applications/malware from establishing outbound connections.

   As far as I can see there are three different possibilities that could reduce the exposure:

   - Change to another personal firewall. Some personal firewalls can provide better protection against threats such as trojans, but cannot be expected to stop all. A new version of Kerio Personal Firewall is being developed, which might be considered at a later date.
   - Adding an application using sandbox techniques, or other programs designed to stop unrecognized code from running, can make it possible to stop most of the threats. The new Tiny Personal Firewall incorporates such technology. This is a sophisticated piece of software, but requires a lot of user interaction to be set up in an efficient manner. Applications like System Safety Monitor or Abtrusion Protector might also be alternatives with functionality that can control code running on a computer.
   - No anti-trojan software is running on the systems at present. Such software could discover and to a certain degree prevent downloading and execution of trojans.

2. *Tighten rules for the LAN in the firewall ruleset (test 18)*

   To tighten the ruleset it is necessary to map exactly what traffic uses the LAN rule. To achieve this it is necessary to log the use of the rule for a period of time. Thru analysis of the log it should be possible to construct a rule that is closer to the minimum of what is actually needed without losing necessary functionality.

   Logging of traffic has been started, but a final result from this task will not be possible to achieve within the time limits of this audit.

3. *System for collecting/analyzing log data from router (test 11)*

   While the router have adequate functionality for generating alarms when suspicious traffic is detected, the capacity to log incidents and keep an adequate audit trail do not meet our standards for compliance the way the router is set up now. Insufficient information about security events makes it much more difficult to trace attacks and the consequences of these attacks. Lack of routines for analyzing logs, and systematic routines cannot be expected in a home office environment, might increase the risk that less visible attacks are not discovered within a reasonable timeframe. The damage could increase when an attack is not discovered within a reasonable amount of time.

Using SNMP to transfer the logs from the router to one of the computers could be a solution to improve the logging of vital information. However this is not certain as such a setup has not been tested. Implementing a solution using SNMP would have a certain cost, especially in relation to the work in planning and implementing a solution.

Of course much of the problem regarding logging is caused by what seems to be a bug in the router's firmware. I hope that the vendor D-Link will issue an update to the firmware for the router that corrects the bug of sending logs by e-mail without a time-/datestamp. The vendor has been notified.

Until the system setup can be changed to improve the logging, heightened awareness of the risks connected to this issue might mitigate the exposure.

3.5. Is the system auditable?

The audit described above has been a strictly technical audit. As explained in relation to assignment 1, the reason the audit was done like this was because organizational and procedural controls are difficult to impose in a home office environment. There usually does not exist written policies and no systematic procedures. It serves no purpose to test controls that you cannot trust to be repeated systematically.

However the human factor is of course important to the security level in a home office environment as well as at bigger offices. As an example we have examined the system's ability to log security events. This has no relevance if no one ever analyses the contents of the logs. I think it is important to emphasize the limitations of this audit. The scope of the audit means that it produces a description of how well the technical perimeter controls function. It does not give an overall view of the security of this environment.

Within the scope of the audit I would say the system is auditable. The audit comprises of tests that for the most part are objective. It was possible to obtain concrete audit evidence for each individual test.

Some of the tests were based on checking parameters set for the router or firewall and did not involve any stimulus/response test. When a test is not verifiable except through the application being audited itself, we presume a trust in that application that an audit ideally should not have to rely on. The audit evidence is stronger if tests can be done independent of the application the audit centers on. For example we have a test above which focus on the router's ability to filter inbound traffic to stop packets with illegal IP addresses. We test this by checking the setup in the router's administrative interface. The audit evidence would have been stronger if a test was performed feeding the router packets with illegal IP addresses and recording the router's response to these. However when conducting an audit we have to operate within a limited timeframe, and checking parameter settings are tests that can be conducted quickly and efficiently. For this audit I think that the most important aspects of the audit were based on stimulus/response tests with strong audit evidence.

The tests in the audit program were based on testing if the functionality in the perimeter defenses worked as they were supposed to, and whether the implementation in this case gave an adequate security level. In a few instances it is possible to question whether the test conducted fully cover the intentions of the control objective specified, as the tests were geared up to available functionality more than the objectives. For example in test no. 1 above the control objective is that only authorized persons should have access to administrative functions for the router. We test this by checking whether a valid password is needed to access the administration interface. We are testing the access control functionality that is actually available in this router, but we are perhaps not fully considering whether this is sufficient to reach the control objective. The tests have been constructed this way because I find it most important to test if the actual available possibilities to secure the systems have been used. These limitations are however discussed in more detail in section 4.4.

I would furthermore like to point out that the audit did not include more detailed analysis of the firewall capability of the router due to a lack of documentation. Being in a home office environment, no policy exists which state what the firewall in the router should protect against. Furthermore the manufacturer, while claiming that the router includes a firewall based on stateful packet inspection[1], provides no details of its abilities. With this background I did not find it possible to identify detailed suitable control objectives and audit items for this particular area. In my opinion further testing in this area would not be an audit, but rather an analysis of the router. It is consequently beyond the scope of this audit to investigate this function in more detail.

[1] The function, which was introduced with in an upgrade of the firmware in 2002 (firmware 1.70b7), is not described in the manual and only a short explanation is given in the help text to the web page. This is the help text available:

"SPI Mode : When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid. ".

4. Assignment 4 – Risk Assessment

4.1. Summary

In general the audit results indicate that the perimeter defenses for the LAN the audit focused on is fairly secure. In particular there are good controls prohibiting access to the LAN from the Internet. However some areas have been discovered where the security could be better. Some of these problems can be fixed quickly with minor corrections and tweaks, but a few require a bit more analysis to find suitable solutions.

When the minor corrections and tweaks have been done, we are left with two issues of particular importance that need to be considered. First and foremost various possibilities must be considered to improve the systems control of outbound connections. The audit proved that rogue applications like trojans could be able to establish outbound connections. To reduce the risk it seems likely that additional software is needed to control more thoroughly what is running on the computers, ref. possible solutions outlined in section 3.4. Secondly there is a problem regarding inadequate routines for handling logs from the router. It is necessary to find a better way to transfer logs from the router to one of the computers on the LAN, probably using SNMP.

I would like to emphasize that the scope of the audit was limited to technical controls of the perimeter defense for this home office environment. This is just one of several areas that need to be audited to gain a full understanding of how secure this network actually is. The conclusions and suggestions from this audit must be seen in conjunction with similar results from other audits of this environment.

4.2. Background/risk

Details regarding the tests that failed and conceived risks associated with the tests can be found in the tables below:

Test 6. Router – remote scan
Results: Nmap scan proved that Port 113 was closed. To be in compliance all ports should be filtered.
Risk: When ports are not filtered, attackers are in a better position to gain valuable information about the router. The information can be used to target specific weaknesses the attacker might be aware of. The attacker could potentially alter router settings, make the router inaccessible, gain access to computers behind the router etc. With only one port not filtered, and with that one being closed, I do not consider the

risk associated with this problem to be very high.

Test 11. Router – log information

Results:
Logs are e-mailed from the router to the administrator frequently as little information can be stored in the router. However the logs that are mailed lack one very important piece of information – date/time of the attack. In addition the information in the logs is not in a form that makes it easy to analyze, not at least because the information is spread out in a number of e-mails.

Risk:
Insufficient information about security events makes it much more difficult to trace attacks and the consequences of these attacks. Recovery could also be more problematical because it would be more difficult to trace events. As a consequence periods of unavailability after security incidents could be longer than otherwise necessary.

Lack of routines for analyzing logs increases the risk that less visible attacks are not discovered within a reasonable timeframe, which could increase the damage such attacks could have.

Test 12. Router – log attacks

Results:
Attacks from the Internet are logged satisfactorily. However successful or unsuccessful attempts to access the router's administration interface are not logged.

Risk:
If an attacker tries to access the router administration to alter rules etc., it is probable that the administrator would not detect this. If the attacker was successful he could allow all traffic to pass thru the router. The LAN behind the router would then be completely open for attacks, bringing on risks of leaking of confidential data, possibilities of using the local network to attack other networks, attacks against the availability of the system etc.

The likelihood of a successful attack using this vulnerability is considered to be low as few people have physical access to the router and remote administration of the router is restricted.

Test 13. Router – firmware

Results:
Audit showed that the router was using firmware 1.80, while version 1.81 was the latest available from the vendor.

Risk:
An attacker could take control of the router by utilizing identified vulnerabilities in older versions of the firmware used by the router.

The risk is considered to be low as the changes from version 1.80 to 1.81 seem to be minimal and do not seem to include any changes based on security concerns.

Test 18. Firewall – Service rules

Results:

Analysis of firewall ruleset indicates that LAN rule allow for more traffic than strictly necessary.

Risk:

The principle of least privileges is broken. If an attacker gains some sort of access to the network, it is a risk that fairly open rules inside the LAN could help the attacker to elevate the attack to the next level. Access to one part of the network, could give a possibility to gain full access to any another part of it.

As the LAN is very small, the vulnerability is not considered a great risk.

Test 19. Firewall – Application rules

Results:

The audit revealed that one application (RealPlayer) was given permission to accept inbound connections, which is not in compliance with the principles outlined in the audit checklist.

Risk: The principle of least privileges is broken, as the application does not seem to need this functionality. As RealPlayer will be listening on certain ports, it might be possible to use vulnerabilities in this application to gain access to the system.

The risk is not considered to be very big because the computer with Kerio Personal Firewall is operating behind a NAT router as a second line of defense, and the vulnerability in itself is not considered to be easy to exploit.

Test 20. Firewall – Leaktests

Results:

The audit revealed that rogue applications trying to make outbound connections from the computers, would not be stopped if they applied more advanced techniques like for example DLL injection. If an application simply tried to make an outbound connection without any attempt of “hiding”, the firewall would stop this and alert the user.

Risk: Rogue applications like trojans could bypass the firewall’s control over which applications are allowed to make an outbound connection. If the trojan manages this there are few limits to the data that can be acquired from our computer (confidential information etc) or data that can be put on to the computer (more malware, storage of files etc.).

Test 21. Firewall – Stop engine

Results:

While it was not possible to stop the firewall manually without knowing the correct password, tests showed that rogue applications could be able to stop the firewall.

Risk:

Rogue applications like trojans could be able to stop the firewall. If the firewall is stopped, there is no control over outbound connections, and rogue applications might transmit any information they want to and from the computer (confidential information, more malware, storage of files, use the computer to attack other machines etc.).

Test 23. Firewall – log
Results: The audit revealed no significant weaknesses in relation to the firewall's logging of specified traffic to and from the computer the firewall is protecting. However successful and unsuccessful attempts to access the firewall administration application do not seem to be logged. Attempts to stop the firewall engine are not logged by the firewall application, but by the operating system as a system event.
Risk: If an attacker tries to access the firewall administration to alter rules etc., it is probably that the administrator would not detect this. If the attacker was successful he could allow all the traffic needed to pass the firewall (e.g. acquiring confidential information, use the computer to attack other computers, send spam to other computers etc.). The likelihood of a successful attack using this vulnerability is considered to be low as few people have physical access to the computers and remote administration of the firewall is restricted.

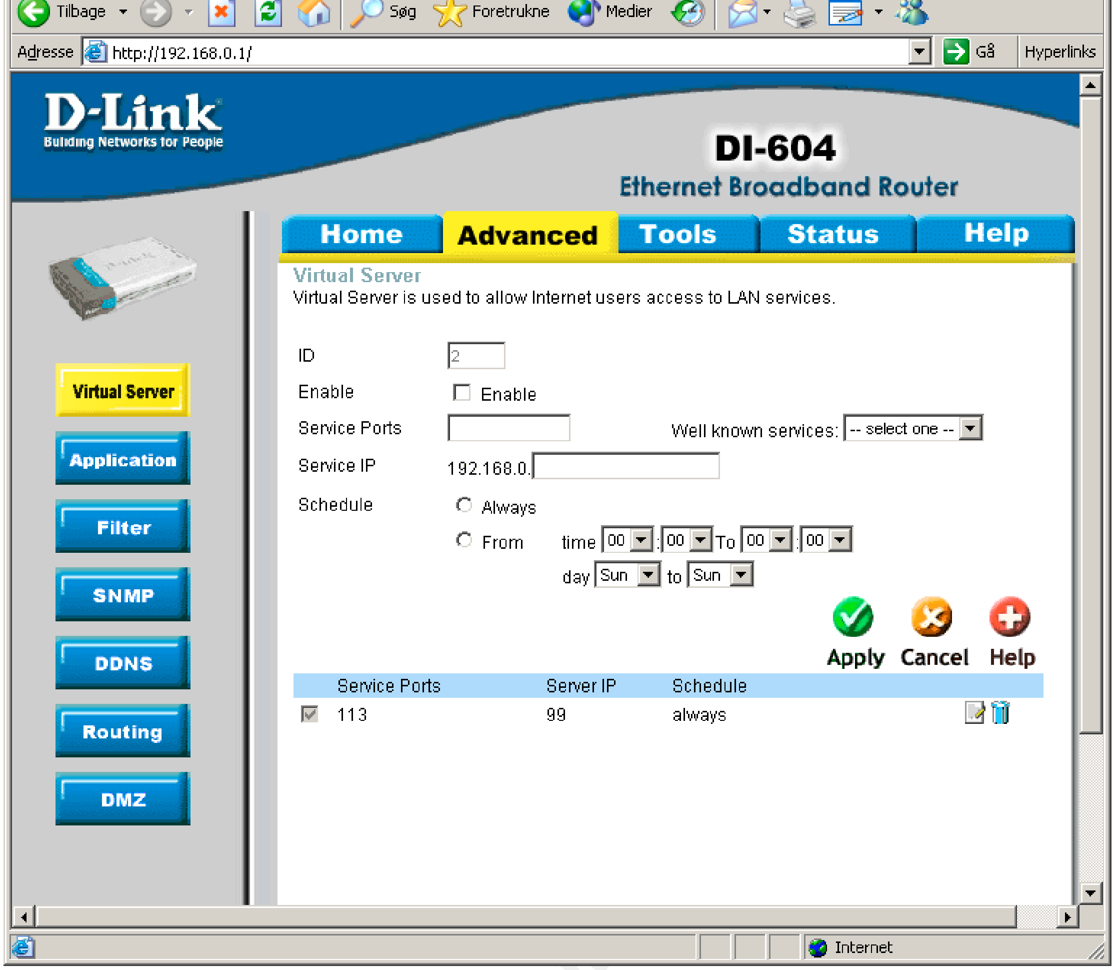
4.3. System changes and further testing

Items where corrective action have been taken:

Test 6 – Router remote scan

Port scanning of the system using Nmap indicated that port 113 on the D-Link broadband router was closed, but not stealthed like all the other ports. While the port is closed and as such not a direct exposure, stealthing the port would make the system less visible. One solution is to forward attempted connections to this port to an unused static IP address on the LAN. That way all attempts to connect to this port would be sent down a "black hole". The router will not respond to the packets.

This screenshot below illustrates the setup in the router administration interface (web page Advanced – Virtual Servers) where packets to port 113 is forwarded to an unused IP address:



Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

ID	2
Enable	☐ Enable
Service Ports	Well known services: -- select one --
Service IP	192.168.0.
Schedule	○ Always
	○ From time 00 : 00 To 00 : 00 day Sun to Sun

	Service Ports	Server IP	Schedule
☑	113	99	always

To test the effect of this I ran a new port scan with Nmap. This was the result of the scan:

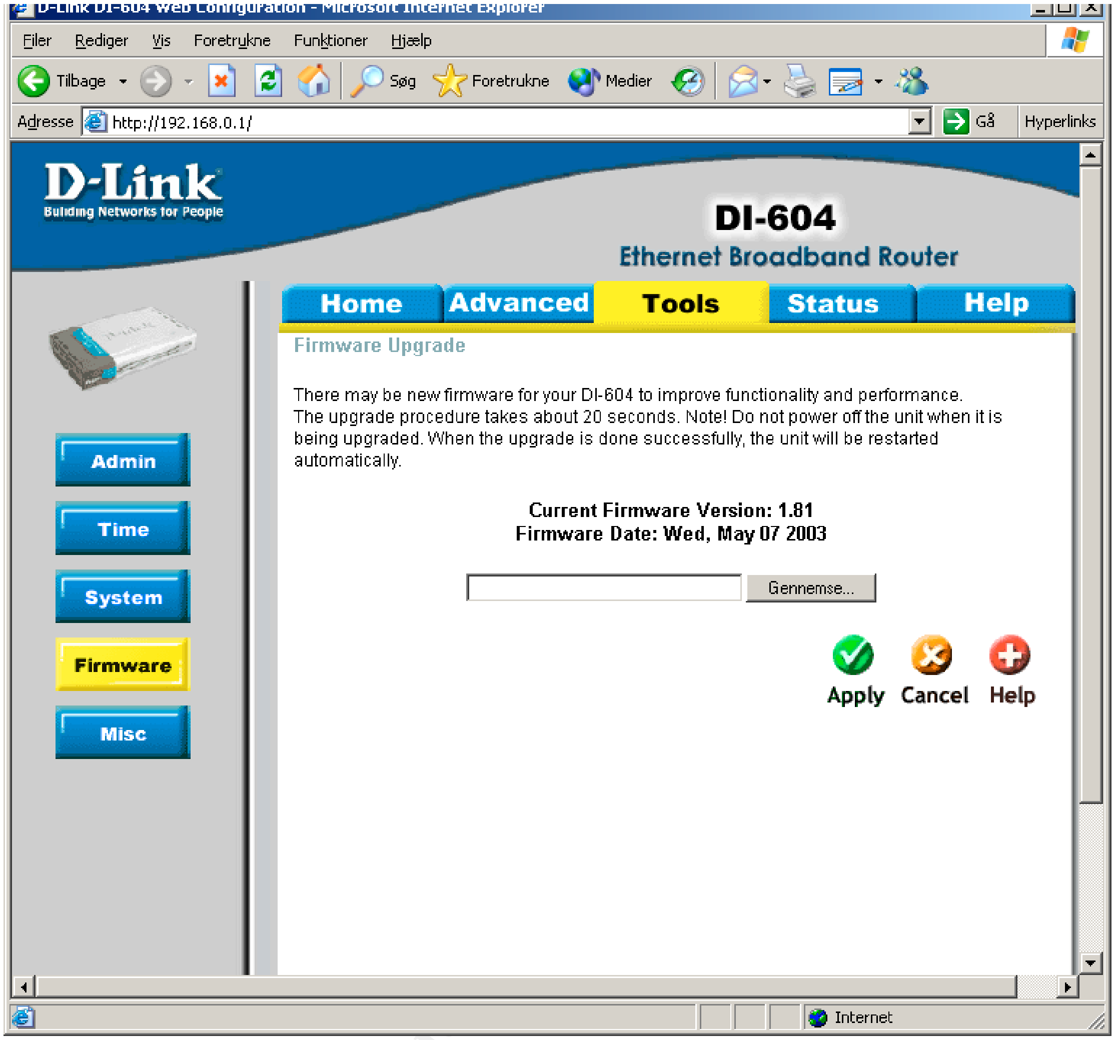
```
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-08-06 22:44 CEST
Host xxxxxxxxxx (xxx.xxx.xxx.xxx) appears to be up ... good.
Initiating Connect() Scan against xxxxxxxxxx (xxx.xxx.xxx.xxx)  at 22:44
The Connect() Scan took 79 seconds to scan 1643 ports.
All 1643 scanned ports on xxxxxxxxxx (xxx.xxx.xxx.xxx) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 79.612 seconds
```

The scan shows that all ports are now considered to be filtered. The tweak served its purpose and the router would now pass the test.

Test 13 – Router firmware

The audit revealed the firmware used in the D-Link broadband router was not the latest available (Firmware 1.80 used, while 1.81 was available). To update the firmware it is necessary to download to a computer on the LAN the newest firmware from D-Link's web site (www.dlink.com.tw). The firmware is installed by either running the exe-file from the computer on the LAN, or accessing the page Tools – Firmware in the administrative interface and specifying the path to the new firmware on the LAN.

The firmware in the router has been updated after the audit. The screenshot below from the router's administration interface show the current firmware being used:


D-Link DI-604 Web Configuration - Microsoft Internet Explorer
Filer Rediger Vis Foretrukne Funktioner Hjælp
Tilbage Søg Foretrukne Medier
Adresse http://192.168.0.1/
Gå Hyperlinks
D-Link
Building Networks for People
DI-604
Ethernet Broadband Router
Home
Advanced
Tools
Status
Help
Admin
Time
System
Firmware
Misc
Gennemse...
Apply
Cancel
Help
Internet

Firmware Upgrade

There may be new firmware for your DI-604 to improve functionality and performance. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

Current Firmware Version: 1.81
Firmware Date: Wed, May 07 2003

Test 18-19 – Firewall ruleset

The audit indicated a few weaknesses in certain rules implemented in Kerio Personal Firewall. As a consequence of the audit a few steps have been taken:

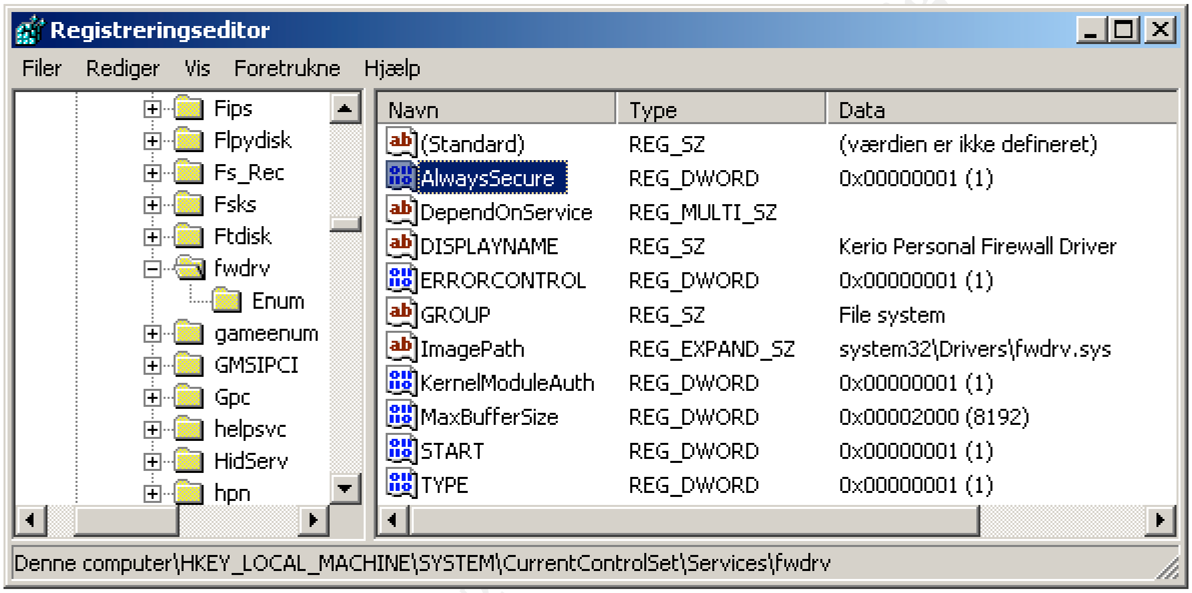
- The rule allowing inbound connections to RealPlayer has been deleted, as the needed functionality in the application does not seem to require such access.
- The utilization of the rule allowing all connections within the LAN is being monitored with the intention of identifying the actual needs for communication and adjusting the rule so that only needed communication is allowed.

Test 21 – Firewall – stop engine

The audit revealed that it would be possible for malware to stop the firewall engine, while leaving the connection to the Internet open for all traffic. Research has revealed a registry tweak that would stop all traffic if the firewall engine stopped (ref.

Broadband reports - Forums - Kerio - Tiny Support, “Registry tweak for Kerio/Tiny” or guide for Kerio Personal Firewall at Optimix.). This is a tweak that is not officially implemented. Using the tweak has a side effect as it makes it almost impossible to use the function for temporarily disabling the firewall, for instance to test something. The tweak also makes it more cumbersome to restart the firewall engine if you do stop it. However there should not be any reason to stop the firewall, so the security gains can be looked upon as bigger than the reduction in functionality.

The tweak involves starting regedit (or any other registry editor) and inserting a DWORD entry “AlwaysSecure” with a value “1” in the key [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fwdrv]. This screenshot illustrates the change:



Navn	Type	Data
(Standard)	REG_SZ	(værdien er ikke defineret)
AlwaysSecure	REG_DWORD	0x00000001 (1)
DependOnService	REG_MULTI_SZ	
DISPLAYNAME	REG_SZ	Kerio Personal Firewall Driver
ERRORCONTROL	REG_DWORD	0x00000001 (1)
GROUP	REG_SZ	File system
ImagePath	REG_EXPAND_SZ	system32\Drivers\fwdrv.sys
KernelModuleAuth	REG_DWORD	0x00000001 (1)
MaxBufferSize	REG_DWORD	0x00002000 (8192)
START	REG_DWORD	0x00000001 (1)
TYPE	REG_DWORD	0x00000001 (1)

Denne computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\fwdrv

After changing the registry I restarted the computer and made sure there was established a connection to the Internet. When running Firewar, the test application claimed that the firewall had been disabled (same message as in original test). Trying to access the firewall’s status window led to the same error message as in the original test. However testing showed that it was not possible to establish any kind of connection to the Internet. When checking running processes on the console, the firewall process still ran.

After adding the value in the registry, the system passed the test as all traffic to and from the machine was stopped when the attempt to stop the firewall occurred.

4.4. System justification

Neither the router nor the personal firewall can log successful or unsuccessful attempts to access their respective administration interfaces (ref. test 12 and 23).

This implies a risk that an attacker could in effect disable all the perimeter defenses and in effect own the systems. However the tests imply that it should not be possible to access the administration interfaces from the Internet, which reduces the risk significantly. Few people have physical access to the local network, which seems to be necessary to exploit the vulnerability. On this background the risks seem acceptable as the possibilities to exploit the vulnerabilities are very slim.

As noted above (section 3.4.) the following issues discovered in the audit remain unresolved for the moment:

1. Rogue applications might be able to make outbound connections (test 20)
2. Rules for the LAN in the firewall ruleset is wider than necessary (test 18)
3. Insufficient log-data is transferred from the router to the computers, and there is no system for analyzing the data (test 11)

The intention of the administrator is to initiate mitigating actions as regards all of these items in due course. As they require some man-hours of work to conclude, they have not been finalized as a part of this audit report. Corrective or mitigating actions for each of the three identified areas of vulnerability have been described in section 3.4. Until all tasks are concluded, the vulnerabilities discovered as part of this audit will continue to exist. The administrator is aware of the risks that these unresolved issues represent, and will take that into consideration in his work. Short-term actions to lower the risk are being considered, for example introducing more stringent rules for downloading files from the Internet for a period of time (ref. danger of infecting the LAN with malicious software).

There are a few areas where the firewall has passed the specified tests, but the tests might have been directed more towards available functionality rather than the idea behind the control objective (ref. section 3.5). This is particularly found in relation to the control objectives for authentication when accessing the administration interface for both the router and the personal firewall (ref. test 1 and 15). Both the router and the firewall have simple authentication mechanisms that consist of one password. There is no user ID and there is no specific requirements for length and complexity of the password, or how often it should be changed. In corporate surroundings the authentication mechanisms cannot be said to be adequate, but in a home office environment with a small network and very few users the risk for unauthorized access is less. Given the local environment for this network, I think the risk of unauthorized access is acceptable and I do not think it is necessary to implement mitigating actions for this problem.

References

Arhont Information Security, “Security issues in D-Link DSL-300/DSL-300G+ Broadband Modem/Router”, March 31, 2003, (URL: http://www.securityfocus.com/archive/1/316951/2003-03-25/2003-03-31/2) (22 August 2003)

Blarp, “Kerio Personal Firewall FAQ”, Updated June 7, 2003 (URL: http://www.blarp.com/faq/faqmanager.cgi?toc=kerio) (22 August 2003)

Boran, Seàn, “ADSL: Security risks and countermeasures”, June 14, 2001 (URL: http://boran.linuxsecurity.com/security/sp/pf/pf_adsl20010614.html) (22 August 2003)

Broadband reports, Security FAQ (URL: http://www.broadbandreports.com/faq/security) (22 August 2003)

Broadband reports - Forums - Kerio - Tiny Support, “Example IP rules” (URL: http://www.dslreports.com/forum/remark,2649460~root=kerio~mode=flat) (22 August 2003)

Broadband reports - Forums - Kerio - Tiny Support, “[Kerio] Generic Rule Set for Kerio (Proxy and no proxy)”, May 3, 2003 (URL: http://www.dslreports.com/forum/remark,6642367~root=kerio~mode=flat) (22 August 2003)

Broadband reports - Forums - Kerio - Tiny Support, “Just one example of rules”, April 19, 2003 (URL: http://www.dslreports.com/forum/remark,2896630~root=kerio~mode=flat) (22 August 2003)

Broadband reports - Forums - Kerio - Tiny Support, “Registry tweak for Kerio/Tiny”, July 9, 2003 (URL: http://www.broadbandreports.com/forum/remark,7309170~root=kerio~mode=flat) (22 August 2003)

Center for Internet Security, “Benchmark for Cisco IOS – Level 1 and 2 benchmarks – Version 2.0”, March 2, 2003 (URL: http://www.cisecurity.org/bench_cisco.html) (22 August 2003)

Charnick, Earl, “Getting the Most Security out of the Linksys® Cable/DSL Router”, Fenbruary 12, 2003 (URL: http://www.sans.org/rr/paper.php?id=619) (22 August 2003)

Core Security Technologies, Advisories, “Vulnerabilities in Kerio Personal Firewall”, April 28, 2003 (URL: http://www.coresecurity.com/common/showdoc.php?idx=314&idxseccion=10) (22 August 2003)

CrazyM, “Customizing Firewall Rules - Application Rules”, October 25, 2002 (URL: http://www.wilderssecurity.com/index.php?board=23;action=display;threadid=4419;prev_next=prev) (22 August 2003)

CrazyM, “Customizing Firewall Rules - Final Block Rules”, October 25, 2002 (URL: http://www.wilderssecurity.com/index.php?board=23;action=display;threadid=4423;prev_next=prev) (22 August 2003)

CrazyM, “Customizing Firewall Rules - Global Permit/Block Rules”, October 25, 2002 (URL: http://www.wilderssecurity.com/index.php?board=23;action=display;threadid=4413;prev_next=prev) (22 August 2003)

CrazyM, “Customizing Firewall Rules - System Wide Rules”, October 25, 2002 (URL: http://www.wilderssecurity.com/index.php?board=23;action=display;threadid=4382;prev_next=prev) (22 August 2003)

dethy@synnergy.net, “Examining port scan methods - Analysing Audible Techniques”, 2001 (URL: http://www.synnergy.net/papers/portscan.txt) (22 August 2003)

D-Link, “DI-604 Express Ethernetwork Broadband Router Manual”, Rev. 102202 (URL: ftp://ftp.dlink.com/Gateway/di604/Manual/di604_manual_204.zip) (22 August 2003)

International Organization for Standardization, ISO/IEC 17799:2000 “Code of Practice for Information Security Management”

IT Governance Institute, “COBIT Control Objectives” 3rd edition, July 2000

Jones, Horace B., “Administratively Auditing the Security Provided by Norton Personal Firewall 2002” (URL: http://www.giac.org/practical/Horace_Jones_GSNA.zip) (22 August 2003)

Kaddouch, Guillaume, “Firewall leak Tester” (URL:http://www.firewallleaktester.fr.st/) (22 August 2003)

Kerio Technologies, “Kerio Personal Firewall 2.1 – User’s Guide”, March 27 2002 (URL: http://www.kerio.com/dwn/kpf/kpf21-en-v1.pdf) (22 August 2003)

Kuhn, Richard, Tracy, Miles C., Frankel, Sheila E., “Security for Telecommuting and Broadband Communication – Recommendations from the National Institute of Standards and Technology” (NIST Special Publication 800-46), August 2002 (URL: http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf) (22 August 2003)

Naidu, Krishni, “Firewall checklist” (URL: http://www.sans.org/score/checklists/FirewallChecklist.pdf) (22 August 2003)

Optimix, "Kerio Personal Firewall" (URL: http://www.optimix.be.tf/) (22 August 2003)

SANS Institute, GIAC System and Network Auditor course book, “Auditing the perimeter”, November 2002

Shackleford, Dave, “Securing the SOHO: A Discussion with a Tutorial of Tiny Personal Firewall 2.0” (URL: http://www.giac.org/practical/Dave_Shackleford_GSEC.doc) (22 August 2003)

Shevelyov, Nicholas, “Auditing Sygate Personal Firewall 4.2” (URL: http://www.giac.org/practical/Nicholas_Shevelyov_GSNA.zip) (22 August 2003)

Spitzner, Lance, “Auditing your Firewall Setup”, December 12, 2000 (URL: http://www.spitzner.net/audit.html) (22 August 2003)

Spitzner, Lance, “Building Your Firewall Rulebase”, January 26,2000 (URL: http://www.spitzner.net/rules.html) (22 August 2003)

Tanase, Matthew, “Always On, Always Vulnerable: Securing Broadband Connections”, March 26, 2002 (URL: http://www.securityfocus.com/printable/infocus/1560) (22 August 2003)

Wack, John, Cutler, Ken, Pole, Jamie, “Guidelines on Firewalls and Firewall Policy – Recommendations of the National Institute of Standards and Technology” (Special publication 800-41), January 2002 (URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf) (22 August 2003)