



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

A Security Checkup For Your Windows at Home

GSNA Practical Assignment
Version 1.2

December 11, 2001

Author: Scott L. Reeder

Table of Contents

1 Introduction	3
Table 1.1 – My Home Computer Systems	3
2 Current State of Practice for Auditing Home Computer Environments	4
2.1 Secure Behavior on the Internet	4
2.2 Acceptable Use Policies	4
2.3 Various Treatments on Securing Your Home Computer Systems	5
2.4 Lists of Steps to Take to Eliminate the Biggest Risks	6
2.5 Analysis of Current Practice	8
2.6 The Audit Checklist	10
2.7 Analysis of Checklist	29
3 Auditing My Home Computer Systems and Network	32
3.1 What is Being Audited	32
Table 3.1 – Risks of My Home Computer Systems	32
3.2 Results from the Audit	33
3.3 Evaluation of Desktop1 System	46
3.4 Evaluation of the Audit Process	48
References	50
Appendix A – Source Code for auditvap.exe	53
Appendix B – Source Code for audituf.exe	54

1 Introduction

Soon after ordering my xDSL service I began to worry about all the security problems coming my way versus my 56K dial-up PPP service. I began to realize how complacent my defenses had become, just because I did not have a ubiquitous presence on the Internet. That was all about to change.

I did not want to cancel my xDSL line since I really wanted to have a faster uplink to the Internet. Oh yeah, I seem to remember promising the rest of my family that with this one xDSL line we could all access the Internet at the same time with our multiple PC's. And what about my neighbors, fiends, and fellow employees? Everyone seemed to be using xDSL and multiple computers networked together with 100BaseT, wireless, or both. It was time I adopted an auditing routine around my systems at home, before a single packet passed through the xDSL modem.

As I considered what my auditing routine might contain, I recalled how we have had difficulty sticking with our routine household chores. The chore of auditing the computer security in our home would fall on my shoulders, for now. Therefore, the steps had to be as objective and automated as possible.

My home computing environment consists of 3 desktop PC's. Below is a table showing the how these systems are setup:

Table 1.1 – My Home Computer Systems

Name	Operating System	Main Applications	Extra Information
Desktop1	Windows 2000 Professional	MS Office 2000 Lots of games	
Desktop2	Windows 2000 Professional	MS Office 2000 Visual Studio VMWare™ 3.0	Can run SuSe Linux 7.2, RedHat Linux 7.1, Windows NT Server, Windows 98 and ME as guest operating systems.
Desktop3	Windows 2000 Server	Routing and Remote Access Service	Provides NAT for the rest. Dual-homed.

In order to keep the scope of this document small, I've intentionally ignored the Linux and VMWare™ 3.0 systems and software.

Desktop3 is a dual-homed system where one of the network cards is connected to the xDSL modem as a DHCP client. My ISP provides me with a static IP address via a variable length subnet mask of 255.255.255.252 and their DHCP server.

2 Current State of Practice for Auditing Home Computer Environments

The current state of checklists and audit procedures for the home environment can be classified as follows:

- Secure behavior on the Internet
- Acceptable use policies
- Various treatments on securing your home computer systems
- Lists of steps to take to eliminate the biggest risks

2.1 Secure Behavior on the Internet

Dr. Sunil Hazari published a three part document that introduces users to secure behavior on the Internet.^{1,2,3} While this series of articles contains similar content to many of the others cited in this writing, Dr. Hazari's tone targets human behavior. For example, users should be aware of the dangers of e-mail attachments, the risks of password theft, and privacy risks of cookies.

Jared M. Anderson has published a curriculum titled "*Ethics in Grade Schools*"⁴ that is apropos to good security habits in the home environment. Anderson describes this curriculum as being designed for 5th graders, which would appear to be an important target age group. "The purpose of this program is to further refine grade schoolers' education on the proper use of computers, both in the classroom and away from school."⁵ Most of my neighbors and colleagues have school age children that have access to at least one home computer. Adults are not immune from needing to be educated on the proper uses of computers. When I asked Mr. Anderson if he thought that the curriculum included in "*Ethics in Grade Schools*" was relevant for adults, he replied "Yes, I certainly do think that the topics I addressed are relevant for adult familiarity/orientation as well, although my examples and [verbiage] were certainly geared toward children."⁶

Then there is the Human Firewall Council and it's web site www.humanfirewall.org. Founded in 2001, this consortium's manifesto is based on the premise that faulty human behavior is the weakest link in computer security and security technology cannot solve all our "infosec" problems.⁷ Of particular interest to secure behavior in the home computing environment is the "Top 10 most common info security mistakes made by individuals" which is based on an article by Alan Horowitz in Computerworld, July 9, 2001 and a press release from the @Stake European office, May 1, 2001.^{8,9} This list shows 9 behaviors that degrade security and 1 that improves it.

2.2 Acceptable Use Policies

My ISP publishes an acceptable use policy under the title of a service agreement. As such, the agreement does not say much about acceptable use. The agreement does say

that I cannot operate an Internet business across the line, and it gives the ISP permission to shut off my e-mail and DSL service if I violate any federal, state, or local laws related to e-mail or the Internet.

Carnegie-Mellon University publishes an acceptable use policy titled “*Statement on Individual Responsibilities in Shared Computing Environments at Carnegie Mellon University*”. This policy provides some general information about topics like:

- Privacy
- Rights and Responsibilities
- Responsible Use of Equipment
- Responsible Sharing of Resources
- Degrees of Improper Behavior¹⁰

This policy references another policy titled “*Carnegie Mellon University Computing and Information Resources Code of Ethics*” which states that all students and faculty have a right to privacy and their fair share of resources. This policy includes statements about user id’s, files, and computer resource consumption.¹¹

Virginia Polytechnic Institute and State University’s “*Policy 2020: Policy on Protecting Electronic Access Privileges*” provides a list of do’s and don’ts related to user accounts and passwords. For example, this policy states that a password should not be easy to guess and should meet some minimum parameters, such as length.¹² Virginia Tech also has a related document titled “*Acceptable Use of Information Systems at Virginia Tech*” which includes guidelines about:

- Protecting your user id and password
- Accessing information that you are authorized to access
- Following copyright laws
- Refraining from cracking passwords
- Using university systems for non-commercial or non-partisan political purposes
- Not creating or propagating viruses or making other non-authorized changes to university data
- Refraining from wasting university computer resources, particularly if it is done intentionally¹³

2.3 Various Treatments on Securing Your Home Computer Systems

There are many writings on securing your computer(s) and network at home. The SANS Reading Room contains papers about home computer security at <http://www.sans.org/infosecFAQ/homeoffice>. In total, these papers suggest the following solutions:

- Firewall, personal or appliance
- Anti-virus software and keep it updated
- Encryption, VPN, e-mail, and e-commerce transactions

- Content filtering, HTTP and e-mail
- Keeping systems updated with the latest patches
- Backup your system(s)
- Disconnecting from the Internet when not using the PC
- Turn off file and printer sharing
- Use long passwords that are hard to guess
- Intrusion Detection System
- Only download files from a trusted source
- Make sure e-mail attachments are scanned for viruses and Trojans
- Remove applications that you don't use
- Make sure all file extensions are visible
- Provide physical security measures
- Perform vulnerability assessment
- Turn off auto-answer mode on your modem^{14,15,16,17}

Bryan Kay Carter published an interesting paper listed in the SANS Reading Room titled "*Security Concerns About Multimedia Technologies*". Carter's writing introduces us to the H.323 and T.120 protocols, which made their way into the mainstream in 1995. Neither of these protocols requires any type of authentication, nor do firewalls handle this type of traffic in an effective manner. If a home computer must use tools like Microsoft's NetMeeting, RealNetworks RealAudio, or CUseeMe Network's CuseeMe software, then you should be aware of the risks. For now, there are very few effective solutions for secure use of multimedia applications.¹⁸

The CERT® Coordination Center publishes an excellent overview titled "Home Network Security" that not only describes many terms and concepts related to computer security at home, but also presents a list of 12 actions that a person can take to mitigate the risks of being on the Internet. This list of 12 actions is much like the list cited above from papers posted in the SANS Reading Room, however the CERT® article adds:

- A reference to the "NeverShowExt" registry value which can be modified in order to disable hidden file extensions. Instructions for modifying this can be found at [URL:http://www.cert.org/incident_notes/IN-2000-07.html](http://www.cert.org/incident_notes/IN-2000-07.html).
- Turn off Java, JavaScript, and ActiveX for both the web browser and e-mail software. This suggestion has a caveat. Disabling Java, JavaScript, and/or ActiveX may reduce functionality.¹⁹

2.4 Lists of Steps to Take to Eliminate the Biggest Risks

Back in 1999, Marc DeBonis published a step-by-step guide titled "Making Microsoft Windows NT 4.0 Server a secure operating system."²⁰ Marc's stated objective of this system is to attempt maximum lock down while still allowing basic TCP and UDP in and out of the application layer of the system. These stepwise instructions start with the initial installation of the operating system and end with the installation of monitoring applications like BackOfficer Friendly and NukeNabber. In between are many steps for:

- Installing all the latest service packs, hot fixes, and patches for NT
- Disabling Netbios services, file and print sharing, and network browsing
- Reducing the risk of SYN flood attacks
- Enabling auditing to the NT event logs
- Setting strong password policies and user rights
- Locking down the Administrator account, Guest account, and the Everyone group
- Disabling unneeded services like spooler and Network DDE
- Disabling DCOM
- Running the C2 configuration utility
- Hardening the system files' ACL's
- Making it harder for a hacker to find the standard .exe's like ftp.exe
- Locking down the floppy drive
- Editing the registry to defend against common exploits

This list also states some usage guidelines for keeping the computer in a maximum lock down state.²⁰

The SANS Institute published a 64 page step-by-step guide to securing Windows 2000 titled, SANS Securing Windows 2000 Step-by-Step Guide. This document provides directions on how to make your Windows 2000 computer secure. (SANS also provides similar documents for Windows NT, Linux, and Solaris. These have been omitted in order to limit the scope of this document to the systems running in my home environment.) In version 1.5 of this document, Jeff Shawgo compiles the contributions from many security professionals into a guide covering the following:

- General Guidelines – best practices of a general nature that should strengthen the security of your computing environment, no matter what version of Windows you are running.
- Securing Data for Physical Transport – focuses on encryption, backups, and recovery features of Windows 2000.
- Security Policy – recommendations on audit policies, user rights, 30 custom security options, disabling unused services, locking down the floppy drive (floplock.exe), and enabling network lockout of the built-in Administrator account (passprop.exe).
- Tools/Utilities – description and use of Microsoft support and resource kit tools, freeware, shareware and some COTS software. Also included is a list of recommendation on custom edits to the Registry to harden the system, but not lock it down as in the case of Marc DeBonis' guidelines cited earlier in this document.
- NTFS Permissions – Access Control Lists for common files, directories, and registry keys.
- Security Configuration Tool – examines the use of templates with the Security Configuration and Analysis Tool (a.k.a. Security Configuration Manager) that comes with Windows 2000.
- Windows 2000 Backup and Recovery – covers ntbackup.exe, emergency repair disks, the recovery console.

- Windows 2000 Active Directory – a high-level discussion on Active Directory.
- Security of Common Applications – a brief look at hardening IIS, Telnet Server, File and Printer Sharing, Windows Services for Unix 2.0, Exchange, Outlook, Outlook Express, SQL Server, and Terminal Services. The hardening steps for IIS are the bulk of this part of the document.

This document includes many detailed recommendations on registry settings, file permissions, and policy settings that are simply too numerous to list.²¹

Steve Elky, of Software Performance Systems, published an article in the SANS Institute Security Digests titled “Automated Auditing in a Windows 2000 Environment” which describes a system for deploying, running, and reporting from an automated Windows 2000 audit.²² While the automation and scripting aspects of this publication are outside the scope of my research, at the heart of Mr. Elky’s systems is a specialized security policy based on an NSA publication titled, “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set”.²³ Mr. Elky also includes the use of SECEDIT, which requires a template file (a.k.a. configuration files). The template file Mr. Elky uses is based on ones published by NSA at: <http://nsa1.www.conxion.com/win2k/download.htm>. This template file implements many of the same recommendations noted in SANS Securing Windows 2000 Step-by-Step Guide in the form of an .inf file that can be used to check the health of security on a Windows 2000 system.

The Center for Internet Security recently published Level One Benchmark Windows 2000 Operating System along with a program that can “score” a Windows 2000 system’s compliance with the benchmarks. This publication also has its roots in the NSA publication cited by Mr. Elky. As a result, the scoring tool uses SECEDIT in a similar fashion to Mr. Elky’s automation system. This scoring tool also includes an evaluation of the level of service packs and hot fixes that have been applied to the system. This is accomplished by using Microsoft’s *hfnetchk.exe* program to get the latest data on service packs and hot fixes. The scoring tool compares the latest service pack and hot fix data to the currently installed updates.²⁴

2.5 Analysis of Current Practice

While there isn’t a shortage of information about securing a home computing environment and securing a Windows NT/Windows 2000 system, there are a number of shortcomings:

1. Usability and Format

This seems to be a major problem with the current state of auditing the security of computers in the home. Even if one can significantly “lock down” one’s home systems using the information contained in the resource cited earlier, the process to follow is not obvious, succinct, or repeatable. Currently, It is just too complicated

and time consuming to audit one's home systems on a regular basis, therefore most systems will remain at risk. One analogy might be changing the oil in one's car. There are a number of steps involved including tracking your miles and disposal. Many Americans find it a challenge to change the oil on their car themselves, even though they know it's an important maintenance item. Given the proliferation of quick oil change services across the United States, only the ones that truly don't care about proper car maintenance fail to have it changed on a regular schedule. Likewise, it would be much better if people had a home security checklist and audit process that could be executed on a routine basis.

The format of the audit document should facilitate a concise and accurate assessment of the home computing environment. Most of the current checklists are lacking in this area. None of the resources cited above provide a document that can enable the auditor to record and "score" the state of the home computing environment.

2. Objectivity

The scoring tool published along with Level One Benchmark Windows 2000 Operating System appears to be a very objective checklist since it is based on computing a score ranging from 0 to 10. The scoring is divided into three categories: "(1) Service Packs and Hotfixes, (2) Policies, and (3) Security Settings."²⁴ However, the publishers of this guide also state, "As time goes on, these allocations are subject to change."²⁴ This may suggest that the scoring tool from the Center for Internet Security is only slightly more objective than the NSA's and Steve Elky's template files for SECEDIT.

The SANS Securing Windows 2000 Step-by-Step Guide is an objective list of things to audit, however even this guide is slanted to locking down Windows 2000 at initial setup versus an assessment against a home computing environment standard.²¹

The rest of the other guidelines and checklists cited in the previous sections do not have any objectivity. For example, having a virus scanning software package installed is a widely accepted practice. Even my father-in-law, an average computer user, knows about viruses and the software that is supposed to stop them. Unfortunately, it seems as if no one publishes a list of steps to follow to check one's current virus scanning software to see if it operating properly. I recently had to spend a day at a friend's home removing a SirCam virus infection. While he had been running virus detection software since day one, he was unaware that his virus definition file(s) were not being updated automatically. His update service subscription expired 3 months prior to this infection. A simple routine of checking the update service's expiration date versus the "last update" date would have prevented this infection and provided value to the virus scanning software.

Not all items in a home computer audit process can be purely objective. One can check the last update date of the virus definition file(s), but what about safe computing behaviors? For example, the Human Firewall Council's "Top 10 most

common info security mistakes made by individuals” says that one should not open e-mail attachments from strangers.⁸ That is an important behavior to assess, but it is difficult to measure objectively. In some cases, these subjective tests can be made more objective versus a simple question with a yes/no type of response. For example, the audit process might ask the home user to describe how he/she reads e-mail with attachments. If the description does not include any narrative on determining the author or origin of the attachment, then perhaps the respondent is unaware of how to practice safe computing, despite being aware of the dangers of e-mail attachments.

3. Applicability to the Home Environment

There are a few recommendations in current practice that are not applicable to the home environment. For example, Marc DeBonis’ “Making Microsoft Windows NT 4.0 Server a secure operating system” states that one should disable DCOM and run the C2 configuration utility.²⁰ Implementing these steps in a home computing environment is overly complex and likely to degrade functionality.

The SANS Securing Windows 2000 Step-by-Step Guide suggests disabling accounts of terminated employees, practicing application recovery, and creating an administrator password control process. These are targeted at an office environment versus a home computing environment. Even a SOHO is not likely to face terminated employee issues.

The acceptable use policies cited in Section 2.2 need to be altered to fit the home environment. Ideally, these altered versions would incorporate both employer or university policies and the unique aspects of general computer use in the home. For example, a policy could state that children under the age of 18 must use a computer in a common area of the home during the hours of 6:00 am to 10:00 pm. This might ensure that a responsible adult can monitor the child’s use of the computer on an ad hoc basis. (i.e., no “secrecy”)

In short, the current checklists need to be more usable, objective, and applicable to the home computer user.

2.6 The Audit Checklist

Below is a checklist for auditing Windows based home network and Windows 2000 systems.

Section 1.0 – Awareness and Behavior

Item	Action	Results	Score
*1.1	Ask, “How do you remember your password(s)?”		
	Describe the answer in the Results column.		

	<p>Score 5 if the answer indicates that the person remembers by use of memory or other mental trick. Mental tricks do not include:</p> <ol style="list-style-type: none"> 1. Writing down in any form. 2. Password derivations that a social engineer might easily attain. (i.e., nicknames, friends/family names, pets names, addresses, phone numbers, and hobbies. 		
*1.2	<p>Ask , “What actions do you take when you walk away from your computer(s) home?”</p> <p>Record the answer in the Results column.</p> <p>Score 5 if answer indicates manual locking of the computer. Score 2 if the screen saver is set to lock the computer after 15 minutes or less.</p>		
*1.3	<p>Ask, “What actions do you take when leaving your computer unattended for 4 hours or longer?”</p> <p>Record the answer in the Results column.</p> <p>Score 5 if the user turns the computer(s) off. Score 2 if the user leave the computer(s) on, but blocks Internet access by:</p> <ol style="list-style-type: none"> 1. Powering off the modem or DSL router. 2. Disconnecting the cable that connects to the public phone switch or neighborhood cable line. 3. Invoking a “no access” feature on the firewall, if present. 		
*1.4	<p>Ask, “What do you do when you receive an e-mail from a stranger?”</p> <p>Record the answer in the Results column.</p> <p>Score 5 if the user deletes it without using a preview pane/view and empties the deleted items from the “trashcan” immediately.</p>		

*1.5	<p>Ask, “What do you do when someone sends you an e-mail with an attachment?”</p> <p>Record answer in the Results column.</p> <p>Score 5 if the user detaches the file, then scans it for viruses before trying to open, and delete any e-mail with an attachment having any of the following attachments:</p> <ol style="list-style-type: none"> 1. .exe, .com, .sys, .bat, .cmd 2. .bas, .chm, .hlp, .lnk, .js, .vbs 3. .pif, .msi, .scr, .url, .vb, .vbe 4. .wsh, .wsc, .wsf 		
*1.6	<p>Ask, “When an Internet site requires you to login and allows you “remember” your account and password, do you enable the “remember me” option?”</p> <p>Record the answer in the Results column.</p> <p>Score 5 if the user does not allow sites to “remember” both account an password. Score 2 if he/she allows accounts to be remembered, but not passwords.</p>		
*1.7	<p>Ask, “True or False, my password for all the Internet sites where I’m required to login, should be the same?”</p> <p>Record True or False in results column. “IDK” if the user does not know.</p> <p>Score 5 if False.</p>		
*1.8	<p>Ask, “True or False, my on-line profile information (which typically includes a credit card number) are safe because I can see the security lock on my browser when using their site(s)?”</p> <p>Record True or False in results column. “IDK” if the user does not know.</p>		

	Score 5 if False.		
*1.9	<p>Run Control Panel, then double-click on the “Add/Remove Programs” icon.</p> <p>Randomly select 5 programs in the “Currently installed programs” list. Ask the user to show you the license for these programs.</p> <p>Record the names of the programs for which a license can be located in the Results column. Remember, some software might be:</p> <ol style="list-style-type: none"> 1. Freeware/Shareware. If so, check to see if the installed copy is registered. 2. Licensed by a soft key versus paper license. <p>Score 1 point for each program that appears to have a proper license.</p>		

Do children under the age of 18 use your computer? (Yes or No)
 (If “no”, then skip to Section 2.0)

Item	Action	Results	Score
*1.10	<p>Ask, “Do the children use the computer(s) in an common area of the home where adults might be able to supervise computer use?”</p> <p>Record Yes or No in the Results column.</p> <p>Score 5 if Yes.</p>		
*1.11	<p>Ask, “Do the children use their real (full) name, phone number, and/or address while using on-line services like:</p> <ol style="list-style-type: none"> 1. Chat 2. Instant messaging 3. E-mail?” <p>Record Yes or No in Results column.</p> <p>Score 5 if No.</p>		

*1.12	<p>Ask, “Have any of your children been given an acceptable use or Internet access policy from their school?” If yes, ask, “Can you show it to me?”</p> <p>Record answers in the Results column.</p> <p>Score 5 if the user can show you a copy of the policy.</p>		
*1.13	<p>Ask, “Have any of the children that are 5th grade or higher ever attended a computer ethics or similar class at their school?”</p> <p>Record Yes or No in the Results column.</p> <p>Score 5 if Yes.</p>		
*1.14	<p>Ask, “True or False, my children are protected from inappropriate content and predators on the Internet because federal, state, and local laws prohibit such things?”</p> <p>Record True or False.</p> <p>Score 5 if False.</p>		

Section 2.0 – Firewall

Do you have a firewall or firewall software in place? (Yes or No)
(If “no”, then go to Section 3.0)

Item	Action	Results	Score
2.1	<p>Go to the following URL: http://scan.sygatetech.com/prequickscan.html</p> <p>Select the “Scan Now” button. Wait for the results.</p> <p>In the results column, summarize how many services are shown to be “blocked”, “closed”, or “open”, respectively.</p> <p>To score this item, use the following formula:</p>		

	<# of blocked> X 5 + <# of closed> X 2		
*2.2	Is your firewall configured to use NAT? (Yes or No) If yes, then score as 5.		

Are you using a personal firewall software package? (Yes or No) For example, ZoneAlarm or Norton Internet Security.
(If “no”, then skip to Section 3)

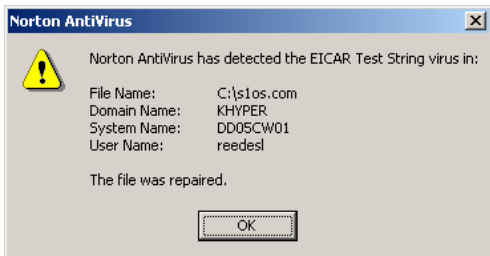
Item	Action	Results	Score
2.3	Ask, “Show me the following settings in your personal firewall product.” a. Logging of alerts (Yes or No) b. Automatic Updates (Yes or No) c. Auto-startup (Yes or No) For each “Yes”, give 5 points, place the sum in the Score column.		
*2.4	Ask, “Show me the programs that are configured inside your personal firewall product.” Add up the number of programs that are set to a. not accept connections from the Internet b. ask before connecting to the Internet (outbound) c. ask before allowing connections from the Internet (inbound) d. connect to the Internet on specific ports (inbound or outbound) Score the with the following formula: The sum of <# of a’s> X 5, <# of b’s> X 5, <# of c’s> X 5, <# of d’s> X 2		

	Divided by the total number of applications listed. Round to the nearest 1.		

Section 3.0 – Anti-virus Software

Do you have anti-virus software installed? (Yes or No)
(If “no”, then go to Section 4.0)

Write down name and version (note: use the “About” dialog):

Item	Action	Results	Score
3.1	<p>Run the auditvap.exe program. (See Appendix A for source code) You should get a response from the anti-virus software similar to this:</p>  <p>The screenshot shows a Norton AntiVirus window with a yellow warning icon. The text inside reads: 'Norton AntiVirus has detected the EICAR Test String virus in:'. Below this, it lists: 'File Name: C:\s1os.com', 'Domain Name: KHYPER', 'System Name: DD05CW01', and 'User Name: reedesl'. At the bottom, it says 'The file was repaired.' with an 'OK' button.</p> <p>Describe the results. If the anti-virus responded to the EICAR Test String with a message saying the files was repaired, then score a 5. If it simply isolated the file in a “quarantine” or just similar, score a 2.</p>		
3.2	<p>Ask, “Show me the date of your virus definitions.”</p> <p>Show results. If the user can show you and that date is within the last two weeks, then score a 5. If the user can’t show you, but the date is still within the last two weeks, then score a 2.</p>		
3.3	Ask, “Show me the automatic update settings.”		

	<p>Show results. If the user can show you and the software is set to automatically update, score with 5.</p> <p>If the user can't show you, but it is set to automatically update, then score 2.</p>		
3.4	<p>Ask, "Show me the last full scan date."</p> <p>Show Results. If scanned within that last 7 days, score 5. If scanned within the last 14 days, score 2.</p>		
3.5	<p>Ask, "Show me your settings for manual scans."</p> <p>Describe the settings in the results column. Score 5 for scanning master boot record. Add 5 if scanning all files, otherwise add 2 if scanning program files and documents only.</p>		
3.6	<p>Ask, "Show me the setting for scanning floppy disks."</p> <p>Describe settings in results. Score 5 if scanning floppy disk on access and shutdown. Score 2 if just scanning floppy disk on access.</p>		

Section 4.0 – Modems

Do you have a modem installed? (Yes or No)

Item	Action	Results	Score
4.1	<p>Go to Control Panel, and double-click the "Phone and Modem Options" icon.</p> <p>Select the "Modems" tab.</p> <p>In the results column, indicate if a modem is installed or not installed.</p> <p>Score 5 if no modem is installed and user answered "no" to question above. Score 2 if a modem is installed and user answered</p>		

	“yes”.		
4.2	<p>Go to Control Panel, and double-click on the “Administrative Tools” icon.</p> <p>Double-click the icon labeled “Services”. Double-click on the service named “Routing and Remote Access”</p> <p>Write the “Startup type” value in the Results column.</p> <p>Score 5 if “Startup type” is set to “Disabled”. Score 2 if “Startup type” is set to “Manual”. Override the 5 or 2 with a 0 if the “Service status” shows “Started”.</p>		
*4.3	<p>Ask, “Do you allow people to connect to your machine remotely via a modem?”</p> <p>Look for software like PC Anywhere or TIMBUKTU.</p> <p>One way to verify this is to ask the user for the phone number that the systems modem is connected to. Then, call that number to see if a modem answers or not.</p> <p>Describe results of your inspection. For example, “No remote access” if user answers “no” and no evidence of dial-in software.</p> <p>Score 5 if “No remote access”.</p>		

Section 5.0 – Encryption

Item	Action	Results	Score
5.1	<p>Go to Control Panel, and double-click the “Internet Options” icon.</p> <p>Select the “Advanced” tab. Scroll down to the section titled “Security.”</p> <p>Record the status (checked or not) of the following items:</p> <p>a. Check for publisher’s certificate</p>		

	<p>revocation.</p> <ul style="list-style-type: none"> b. Do not save encrypted pages to disk. c. Use PCT 1.0 d. Use SSL 2.0 e. Use SSL 3.0 f. Use TLS 1.0 g. Warn about invalid site certificates h. Warn if changing between secure and not secure mode <p>Score 5 if “a” is checked. Add 5 if “b” is checked. Add 5 if “e” is checked while “c”, “d”, and “f” are not checked. Add 5 if “g” is checked. Add 5 if “h” is checked.</p>		
*5.2	<p>Ask, “Can you digitally sign and encrypt your e-mail?” If yes, then ask, “Show how you do that by sending an encrypted and signed e-mail to him/her self.”</p> <p>Describe what you see in the Results column.</p> <p>Score 5 if the user is able to sign and encrypt e-mail.</p>		
5.3	<p>Start Internet Explorer.</p> <p>Select the “Help” and “About” items from the menu.</p> <p>Record the value show for the cipher strength in the results column.</p> <p>Score 5 if the cipher strength is set to 128-bit.</p>		
*5.4	<p>Ask, “Do you encrypt valuable data on your disk?” If yes, then ask, “Show me how you do that?”</p> <p>Describe what you see in the Results column.</p> <p>Score 5 if the user can encrypt valuable files on the disk.</p>		

Section 6.0 – Content Filtering

Do you have content filtering software installed? (Yes or No)

Item	Action	Results	Score
6.1	<p>Point your browser to http://www.weather.com.</p> <p>If you get 2nd browser window advertising some product, record “ads not blocked” in the Results column, otherwise record “ads blocked”.</p> <p>Score 5 if “ads blocked”.</p>		
6.2	<p>While on the www.weather.com home page, select the “File” menu.</p> <p>Find the menu item that allows you to send the entire page as an e-mail.</p> <p>Send the e-mail to yourself.</p> <p>When you receive the e-mail, try to read it.</p> <p>Describe what happens in results.</p> <p>Score a 5 if the user is unable to read all the content from the e-mail message that was on the home page inside the browser.</p>		
*6.3	<p>Ask, “Is your content filtering software configured to stop access to adult content web sites?”</p> <p>Record the answer in the results column.</p> <p>Score 5 if the answer is “yes”.</p> <p>Note: If you have written agreement stating that you are allowed to test for filtering of adult content, you may want to verify the user’s answer to this question by attempting to connect the user’s browser to a “test” web site.</p>		

Section 7.0 – Intrusion Detection

Do you have network intrusion detection software/appliance in place? (Yes or No)

(If “no”, then skip 7.1 and 7.2)

Item	Action	Results	Score
7.1	<p>Go to the following URL: http://www.khyper.com/a.ida?AAAAAA</p> <p>Ask the user to show you the alert log of the intrusion detection sensor.</p> <p>Indicate whether the sensor detected a web attack to an IIS ISAPI program.</p> <p>Score a 5 if the log show something similar to the following from a default SNORT rule set: [**] [1:1243:2] WEB-IIS ISAPI .ida attempt [**] [Classification: Web Application Attack] [Priority: 1] 12/07-16:18:51.707360 <user’s ip address>:<some port #> -> 64.225.154.175:80 TCP TTL:127 TOS:0x0 ID:14771 IpLen:20 DgmLen:398 DF ***AP*** Seq: 0x7F3A9464 Ack: 0x2765B038 Win: 0x10C0 TcpLen: 20 [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=can-2000-0071] [Xref => http://www.whitehats.com/info/IDS552]</p>		
*7.2	<p>Ask, “Show me some of the rules on the IDS sensor.” Ask, “Can you tell me what any of these rules are supposed to detect?”</p> <p>Record the name and version of the IDS sensor in the results column.</p> <p>Score 5 if the user can show you a rule and explain its purpose. Score a 2 if they can show you the rules, but are unable to explain any of them. (one accurate explanation is good enough)</p>		

Do you have host-based intrusion detection software in place? (Yes or No)

(If “no”, then skip to the next section)

Item	Action	Results	Score
7.3	Try to login to the system with an incorrect		

	<p>username and password 5 times.</p> <p>Ask the user to login with a legitimate user account and password.</p> <p>Ask the user to show you the alert logs of the host-based IDS.</p> <p>Score 5 if the alert is displayed automatically as a “pop-up dialog”. Score 2 if the user can show you an alert in the log saying that some false user was trying to log into your system, but it does not automatically pop-up an alert dialog.</p>		

Section 8.0 – Strong Passwords

Strong passwords are also evaluated and scored under Section 13.0, below.

Item	Action	Results	Score
8.1	<p>Start Control Panel. Double-click the “Administrative Tools” icon. Double-click the “Computer Management” icon.</p> <p>Expand the tree named “Local Users and Groups”, and then select the tree node named “Users”.</p> <p>Select the guest account. (may not be called “Guest”) Try to set the password for the guest account to “password”. If you can’t use this password, then add numbers and special characters to the end of “password” until you get a password that is allowed.</p> <p>Score a 5 if you have to add at least one special character and at least one number to the end. (i.e., passwords have to be at least 10 characters in length and be “complex”).</p>		

Section 9.0 – Multimedia and Related Applications

Item	Action	Results	Score
*9.1	Ask, “Do you use any software that allows		

	<p>you to access music, video, or live broadcast content over the Internet?”</p> <p>(Common applications might be Real Player or Napster)</p> <p>Record all the names in the Results column.</p> <p>Score a 5 if the user does not use such software.</p>		
*9.2	<p>Ask, “Do you use any software that allows you to upload or share data with others on the Internet?”</p> <p>(A Common application might be Gnutella or NetMeeting)</p> <p>Record all the names in the Results column.</p> <p>Score 5 if the user does not use such software.</p>		
*9.3	<p>Ask, “Do you use any software that allows you to do video conferencing and/or voice communications over the Internet?”</p> <p>(Common applications might be Dialpad, Net2Phone, Interwise, or NetMeeting)</p> <p>Record all the names in the Results column.</p> <p>Score 5 if the user does not use such software.</p>		
*9.4	<p>Ask, “Do you use any chat software?”</p> <p>Record all names in the Results column.</p> <p>Score 5 if the user does not use such software.</p>		
*9.5	<p>Ask, “Do you use any software that allows you to play games with other people over the Internet?”</p>		

	Record all names in the Results column. Score 5 if the user does not use such software.		

Section 10.0 – Unused Software

Item	Action	Results	Score
10.1	Run the audituf.exe program. Record the total number of EXE's, Un-used EXE's, and OS2/POSIX files reported by audituf.exe. Write the audituf.exe score in the Score column.		

Section 11.0 – Special Administration Accounts

Item	Action	Results	Score
11.1	Start Control Panel. Double-click the “Administrative Tools” icon. Double-click the “Computer Management” icon. Expand the tree named “Local Users and Groups”, and then select the tree node named “Users”. Examine the contents of the right side pane. Record the names of the built-in Administrator and Guest accounts. Ask the user to help you find these two names. Score 5 points if the built-in Administrator and Guest accounts have been renamed, and the renamed Guest account is disabled. Score 2 if the two accounts have been renamed, but the Guest account is disabled.		
* 11.2	Ask the user to show you what account he/she usually logs in with to do non-administration related work.		

	<p>Show the properties of that account, and then select the “Member of” tab.</p> <p>Record the groups that this account is a member of in the results column.</p> <p>Score a 5 if this user account is not a member of the Administrator group or a group that has administrative authority on the system.</p>		
11.3	<p>Ask, “Have you run the passprop.exe program on this system?”</p> <p>If so, run again without any options. Record the results in the results column.</p> <p>Score 5 if the Administrator account can be locked out.</p>		
11.4	<p>Start Control Panel. Double-click the “Administrative Tools” icon. Double-click the “Services” icon.</p> <p>Look for the floppy lock service (floplock.exe).</p> <p>Score 5 points if the floppy lock service is installed, running, and set to start automatically. Score 2 point if the floppy lock service is installed, running, and set to start manually.</p>		

Section 12.0 – Patches and Services Packs

Item	Action	Results	Score
12.1	<p>Go to the following URL: http://windowsupdate.microsoft.com</p> <p>Select the “Product Updates” link. Wait for the results. (let the Windows Update ActiveX control install)</p> <p>In the results column, list any Critical Updates and Service Packs needed. Also, list any Advanced Security Updates needed.</p>		

	<p>Score 5 if no Critical Updates, Services Packs, or Advanced Security Updates are listed.</p> <p>Note: The scoring tool used in the next section will all evaluate Service Packs and Hot Fixes.</p>		
12.2	<p>Go to the following URL: http://office.microsoft.com/productupdates</p> <p>Wait for the results. (let the Windows Update ActiveX control install)</p> <p>In the results column, list any Updates and Service Packs needed.</p> <p>Score 5 if Updates or Services Packs are listed.</p>		

Section 13.0 – Hardened Systems

Item	Action	Results	Score
13.1	<p>Install the Windows 2000 Level 1 Score Tool. http://www.cisecurity.org/bench_win2000.html</p> <p>Run the tool using the w2k_workstation.inf, w2k_server.inf, or w2k_dc.inf template as appropriate for the system.</p> <p>Record the scores, including the overall in the results column. Also, make note of any Hot Fixes that are needed by listing the MS bulletin tag and “Q” tag.</p> <p>Score the results using the following formula. <overall score> X 10</p>		

Section 14.0 – Macro Protection

Do you any Microsoft Office software installed? (Yes or No)
 (If “no”, then skip to the next section)

Item	Action	Results	Score
14.1	<p>If you have MS Word installed, select the “Tools”, “Macro”, “Security” menu items.</p> <p>Record the security level in the Results column, and if there is virus scanning installed or not.</p> <p>Score 5 if level “High”, 2 if level “Medium”. Add 5 if virus scanning is installed.</p>		
14.2	<p>If you have MS Excel installed, repeat the same steps as 14.1.</p>		
14.3	<p>If you have MS Powerpoint installed, repeat the same steps as 14.1.</p>		

Section 15.0 – Backups

Item	Action	Results	Score
*15.1	<p>Ask, “Tell me how you backup the key files on your system?”</p> <p>Describe the answer in the Results column.</p> <p>Score 5 if the user can accurately describe a reasonable backup process.</p>		
*15.2	<p>Ask the user for the latest backup set. Ask, “How often do you backup the critical files on your system?”</p> <p>Describe the media and frequency of backups in the Results column.</p> <p>Score 5 if the media is tape or CD-ROM/DVD and the latest backup is within the last 30 days.</p>		
*15.3	<p>If the user uses encryption, ask, “Do you backup your encryption keys?” If the user answers yes, ask, “Show me how you do that.”</p> <p>Record the description of how this is</p>		

	performed by the user. Score 5, if you are able to verify that the user is successfully backing up encryption keys.		
*15.4	Ask, "Tell me how you restore the key files to your system?" Describe the answer in the Results column. Score 5 if the user can accurately describe a reasonable restore process.		

Section 16.0 – Physical Data Security

Item	Action	Results	Score
16.1	Check the BIOS setting to see if the system is set to boot from the hard drive first. Record the setting in the Results column. Score 5 if system is only set to boot from the hard drive. Score 2 if set to boot from hard drive first, then other drive media (i.e., floppy or CD) after that.		
16.2	Reboot the machine to see if a password is required to proceed by either the BIOS or OS. Record condition in Results. Score 5 if required by OS (due to SYSKEY settings), else 2 if by the BIOS.		
*16.3	Are the backup media stored in a safe place? Describe how they are stored. Score 5 if stored in a locked container, safe, or similar lock box. Add 5 if also stored off-site in a secure place like safe deposit box at a local bank.		

Section 17.0 Add Up Scores

Add up the scores per section, and then add all the section totals to get a grand total.

Section Name	Score
Section 1.0	
Section 2.0	
Section 3.0	
Section 4.0	
Section 5.0	
Section 6.0	
Section 7.0	
Section 8.0	
Section 9.0	
Section 10.0	
Section 11.0	
Section 12.0	
Section 13.0	
Section 14.0	
Section 15.0	
Section 16.0	
Grand Total	

2.7 Analysis of Checklist

The scoring system of the checklist in *Section 2.6* is designed to allow for additional test items over time. Therefore, the Grand Total is not an absolute measure. For example, if a new test is added to *Section 14.0*, then the maximum possible points for that section and the Grand Total increases by at least 5. However, that specific test may or may not be a factor in determining if the system is outside acceptable risk. This one new test may only provide a means to measure if the system is continuing to improve protection, beyond a minimum standard. On the other hand, a system that fails a single critical item should be considered “out of spec”. Finally, the scores are really just summarization of the individual tests. If one does not understand the reason for obtaining or not obtaining a specific score, then the scores are meaningless.

The following table lists the minimum number of points per section of the checklist that a system must score, else be rated “out of spec”:

Section Name	Minimum Score	Why
Section 1.0	15	User should have some

		basic awareness of computer security.
Section 2.0	30	A firewall should be in place. If there is one, it should be able to block most everything in the scan. If not, it's really worthless.
Section 3.0	20	Any home system had better have virus software that is working.
Section 4.0	5	If a modem is installed, it should not be allowing remote dial-in access.
Section 5.0	5	Encryption is mainly bonus points for a home system, but having the browser settings correct is a minimum requirement.
Section 6.0	0	Content filtering is mainly bonus points, however blocking this will help prevent some worms.
Section 7.0	0	All bonus points. IDS is too complex for most users in the home.
Section 8.0	5	Must have strong passwords. Weak ones make all other defenses useless.
Section 9.0	0	All bonus points. This minimum is likely to change over time.
Section 10.0	5	You get 5 just by removing OS2 and Posix subsystems.
Section 11.0	5	This is like weak passwords. The built-in accounts have to be renamed.
Section 12.0	5	Have to have the system patched and up-to-date.
Section 13.0	50	Any home system should be hardened enough to keep the script kiddies out.
Section 14.0	15	Must be protected against macro viruses. If the system does not have MS Word, Excel, or PowerPoint

		installed, then the minimum for this is 0.
Section 15.0	5	At least if it's backed up someone else can try to get it restored.
Section 16.0	0	Bonus points for the person that does these.

Any system that has any section that does not meet the minimum scores show above it to be flagged as “out of spec”.

Also, any of the items listed in the checklist where the item number is preceded with an asterisk are subjective. Therefore, one has to evaluate these as best as one can.

© SANS Institute 2000 - 2002, Author retains full rights.

3 Auditing My Home Computer Systems and Network

3.1 What is Being Audited

As stated in the Introduction, I am auditing my home computer systems and networking environment that is always connected to the Internet. My home computing environment consists of 3 desktop PC's, a 10/100 5-port hub, and DSL modem. Below is a table showing the risks associated with 3 desktop PC's:

Table 3.1 – Risks of My Home Computer Systems

Name	Operating System	Main Applications	Risks
Desktop1	Windows 2000 Professional	MS Office 2000 POP3 client Internet Explorer Lots of games	This machine is at high risk of getting a virus or worm. The children's games might present a risk to crashing the system. This system is used by children under the age of 18 browsing the Internet for school assignments; therefore, any adult content, chat, or advertising would be inappropriate.
Desktop2	Windows 2000 Professional	MS Office 2000 Visual Studio VMWare™ 3.0	Sensitive financial data located on this machine. Has a compiler loaded, so if the hacker gets to this machine it would be too easy to hide. Lots of e-mail and web browsing, therefore risk of virus or worm is high. VPN access to work, therefore system integrity has to be very high at all times.
Desktop3	Windows 2000 Server	Routing and Remote Access Service Snort Internet Explorer	Directly connected to the Internet, therefore the first place of attack. Risk of worms.

Desktop3 is a dual-homed system where one of the network cards is connected to the xDSL modem as a DHCP client. My ISP provides me with a static IP address via a variable length subnet mask of 255.255.255.252 and their DHCP server.

The audit checklist is structured into sections that represent various layers of security that need to be evaluated. Sections 1.0, 2.0, and 7.0 are not specific to each of the PC's in Table 3.1. The other sections are audited and evaluated for Desktop1 from the table above. Also, the checklist instructs the auditor to ask the user questions. Since I'm the auditor and the user, I will be asking those questions to myself.

3.2 Results from the Audit

Section 2.0 – Firewall is an important part of the layers of defense in my home network. As one will see in the following screen shots, Norton Internet Security is installed as a personal firewall on Desktop1. In addition, Desktop1 routes all Internet traffic via Desktop3, which is running Zone Alarm as an ICS Gateway. Below are the results of running the tests in Section 2.0 (4 specific tests).

Test results from 2.1:

Your system ports are now being scanned and the results will be returned shortly...
Results from **quick scan** at TCP/IP address: **64.137.203.161**

Ideally your status should be "**Blocked**." This indicates that your ports are not only closed, but they are completely hidden (**stealthed**) to attackers.

Additional Information			
			Used by FTP for data transmission in P
			File Transfer Protocol is used to transfer computers. A misconfigured FTP server attacker to transfer files, trojan horse programs at will.
			Secure Shell, a encrypted type of misconfigured it can allow for brute-for your administration account
			Telnet is used to remotely create a shell this can allow an attacker to control you he was sitting in front of it
			SMTP is used to send email across the allows an attacker to verify user account system, send anonymous (spam) email, files on your hard drive.

			Domain Name Services are used to resolve domain names to IP addresses.
			Used mainly by file transfer and chat.
			Finger offers information about who is logged in to your computer.
			HTTP web services publish web pages. A misconfigured web server can not only be exploited by an attacker needed information about his target, but also allow for various security breaches.
			Post Office Protocol is used to receive email. It is often used by attackers to create fake email accounts, execute programs, and even intercept email.
			Ident is often used for IRC (chat), but it can also be used to get information about your system and who is logged in.
			NetBios is used to share files through a Local Area Network Neighborhood. If you are connected to a network with this open, you could be sharing your hard drive with the world! This is a very dangerous service to have open.
			Secure Web Servers are often used by companies to host their online vendors.
			In Windows 2000, Microsoft added the ability to run SMB directly over TCP/IP, without the need for NBT.
			Socks Proxy is an internet proxy service. If you are using servers will not allow you to log in if you are not using an unsecured socks proxy.
			HTTP Web Proxy allows other people to use your web browser off of your computer to forward traffic to web servers.

Results from scan of **commonly used trojans** at TCP/IP address: **64.137.203.161**

			Possible Trojans
			BackDoor-G, SubSeven, SubSeven A

			BackDoor, TtansScout
			BackDoor-G, SubSeven
			Back Door Setup, ICKiller
			GabanBus, NetBus, Pie Bill Gates
			Baron Night, BO client, BO2, Bo Fac Back Orifice, DeepBO
			Back Orifice 2000
			School Bus, Back Orifice 20

Results from scan of **ICMP** at TCP/IP address: **64.137.203.161**

			Additional Information
			ICMP ping request. ICMP is used to machine in order to test internet

To test for NAT (Item 2.2), I went to a command prompt and type “ipconfig /all” and piped the output to a text file. The resulting text file is:

Windows 2000 IP Configuration

```
Host Name . . . . . : Desktop1
Primary DNS Suffix . . . . . :
Node Type . . . . . : Mixed

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : Network Everywhere Fast Ethernet
Adapter (NC100 v2)
Physical Address. . . . . : 00-20-78-05-43-39

DHCP Enabled. . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IP Address. . . . . : 10.10.69.171

Subnet Mask . . . . . : 255.255.255.0
```

```

Default Gateway . . . . . : 10.10.69.69

DHCP Server . . . . . : 10.10.69.69

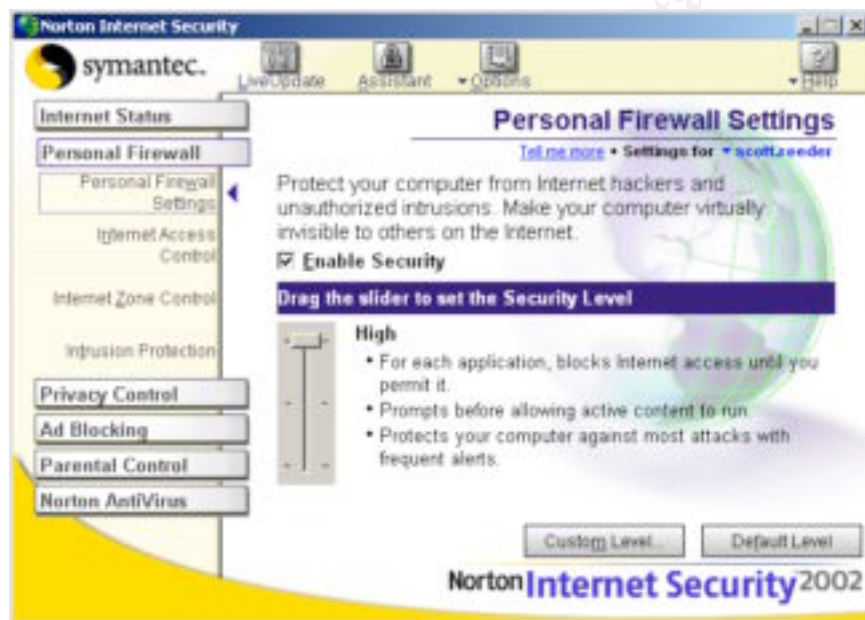
DNS Servers . . . . . : 10.10.69.69
Lease Obtained. . . . . : Wednesday, December 12, 2001 3:36:11
PM

Lease Expires . . . . . : Wednesday, December 19, 2001 3:36:11
PM

```

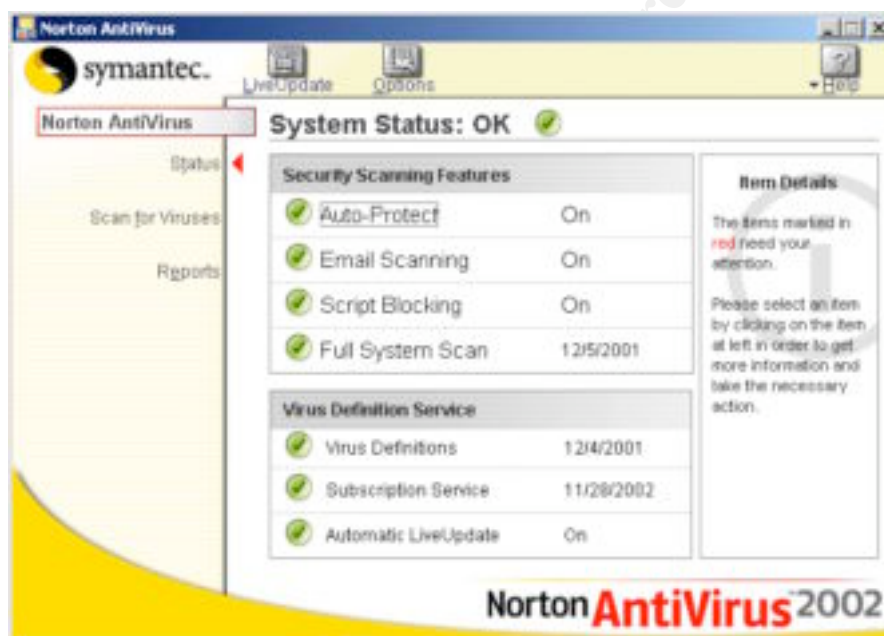
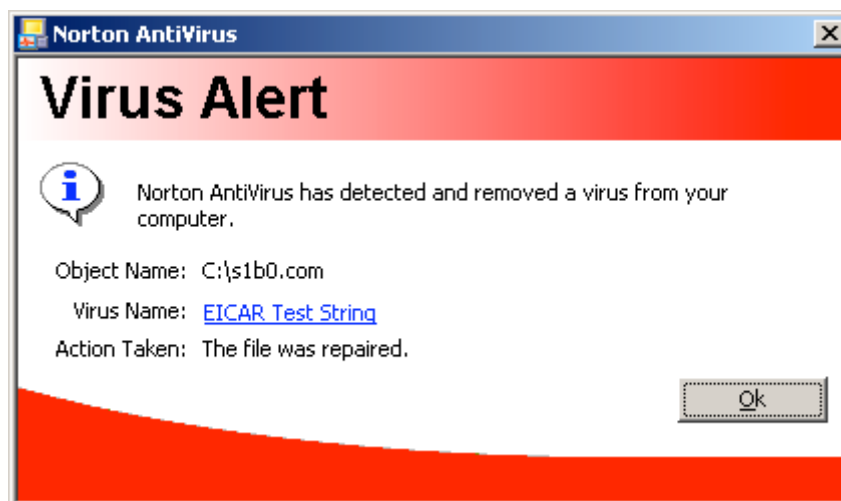
One can compare the address information from the “ipconfig /all” command to the address indicated in the scan done in test 2.1 to see if NAT is in place.

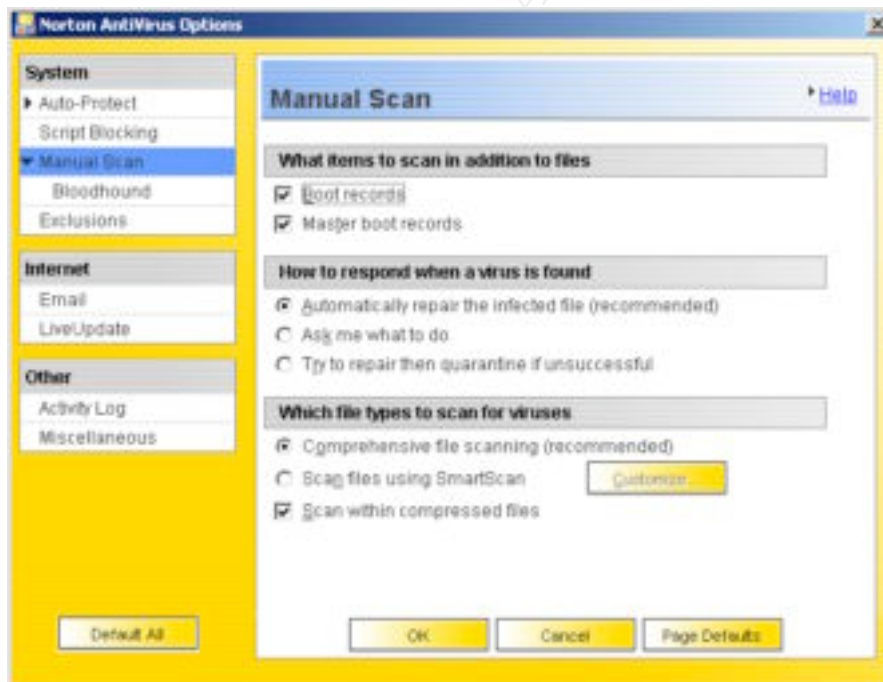
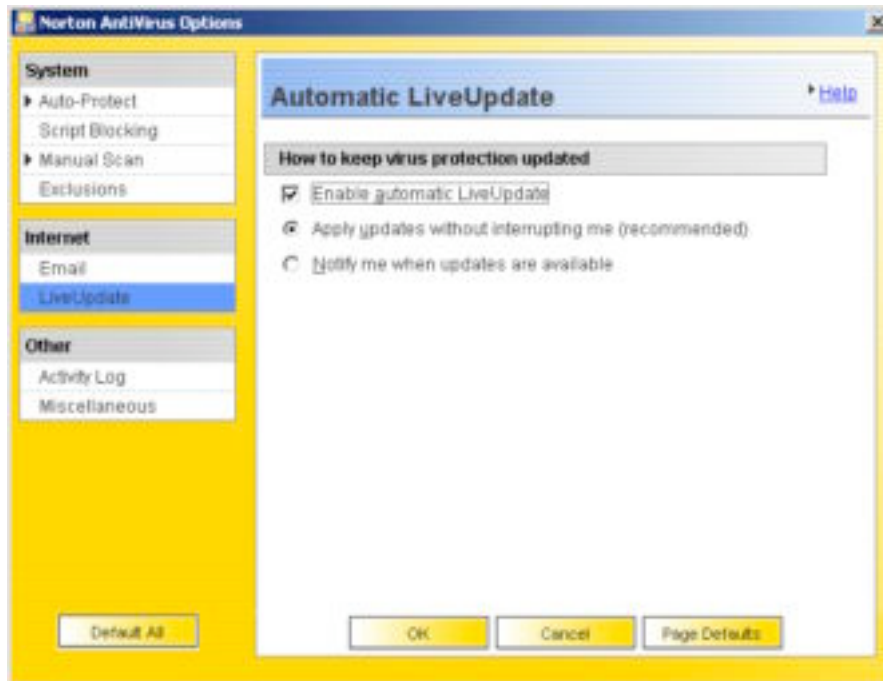
By accessing the configuration option on the personal firewall on Desktop1, the following screen shots were captured:

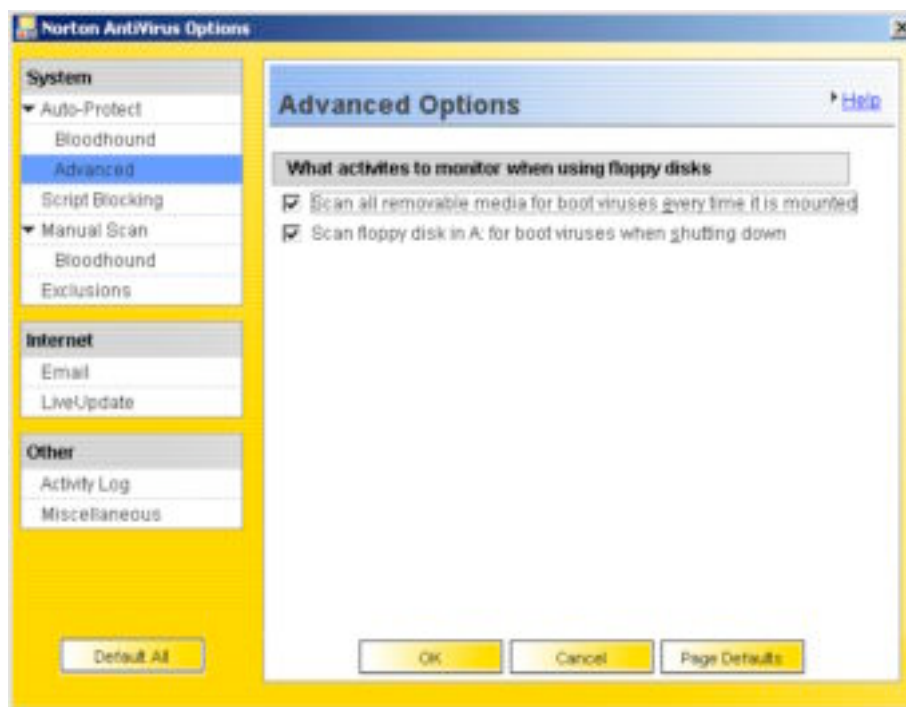




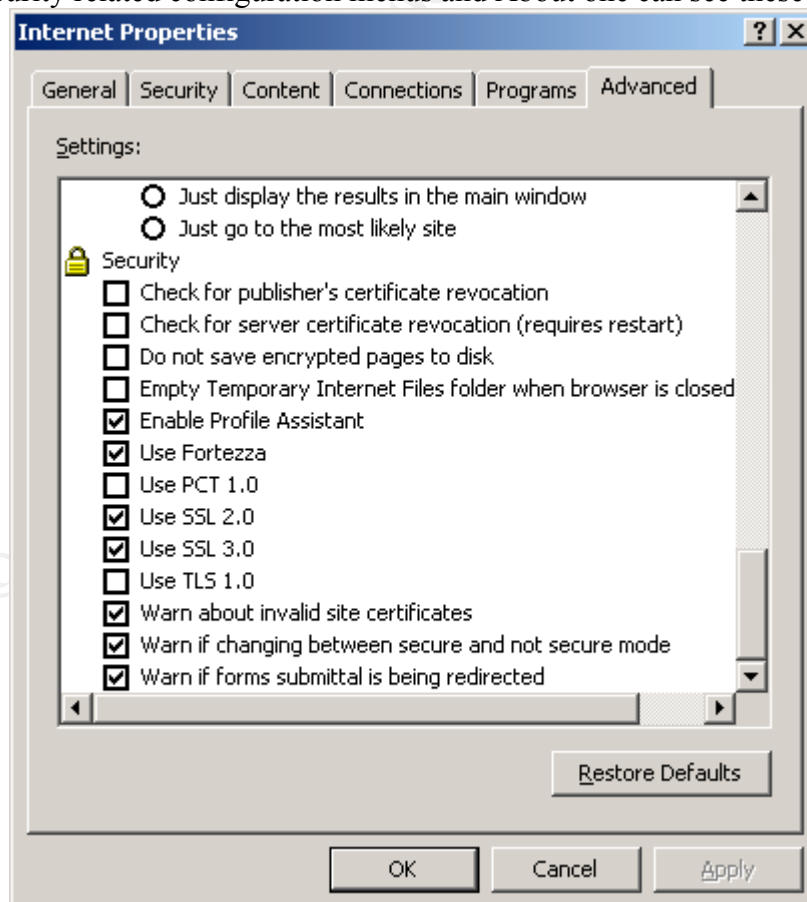
Section 3.0 – Anti-virus Software is critical to having a secure computing environment on Desktop1. By following the steps outlined in the individual tests under Section 3.0, the following information was gathered:







Section 4.0 – Encryption deals with some important SSL setting for the browser, so by using the security related configuration menus and About one can see these settings.





Section 6.0 – Content filtering is very important on Desktop1 because children under the age of 18 frequently use it to do homework assignments. By following the steps shown in items 6.1 through 6.3, it was determined that most advertising was blocked and HTML embedded into an e-mail message was not allowed back out to the originating web site. In addition, when trying to access a known adult content web site, the following was displayed in the browser.

Norton Internet Security 2002 has blocked access to this restricted site

Site: <http://www.whitehouse.com/>

Blocked categories: Sex/Acts

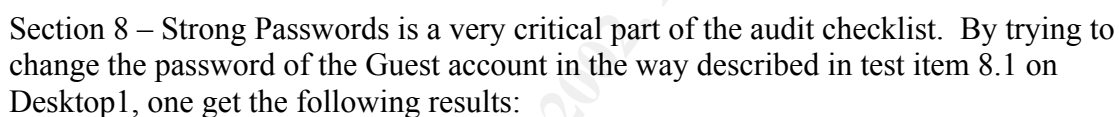
If you think this Web site is incorrectly categorized, visit the Symantec Internet Security Center to report it.

Section 7.0 – Intrusion Detection is a valuable tool in the home network environment because it can log most suspicious activity. However, it must be working properly. Test item 7.1 generated the following entries in the alert.ids file where the Snort sensor runs:

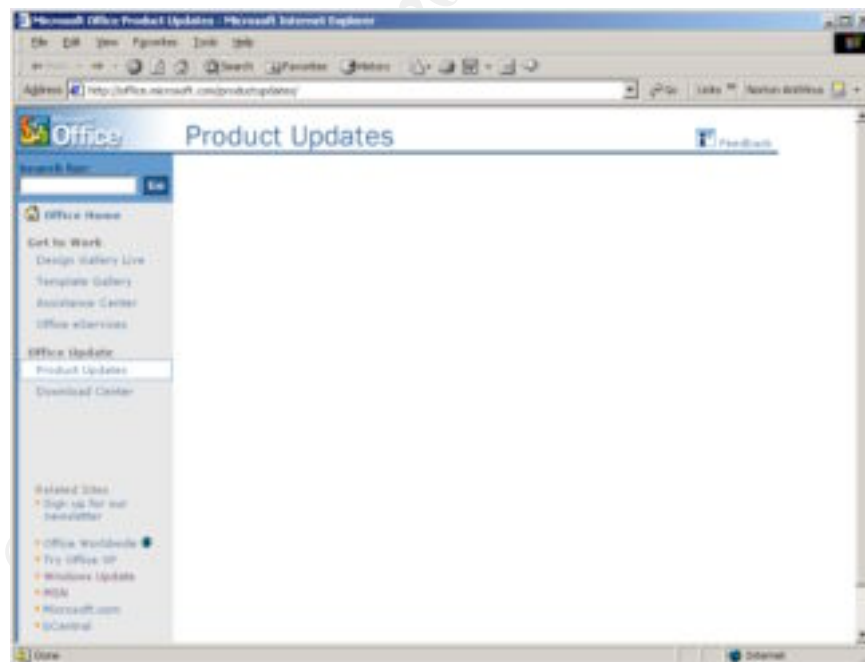
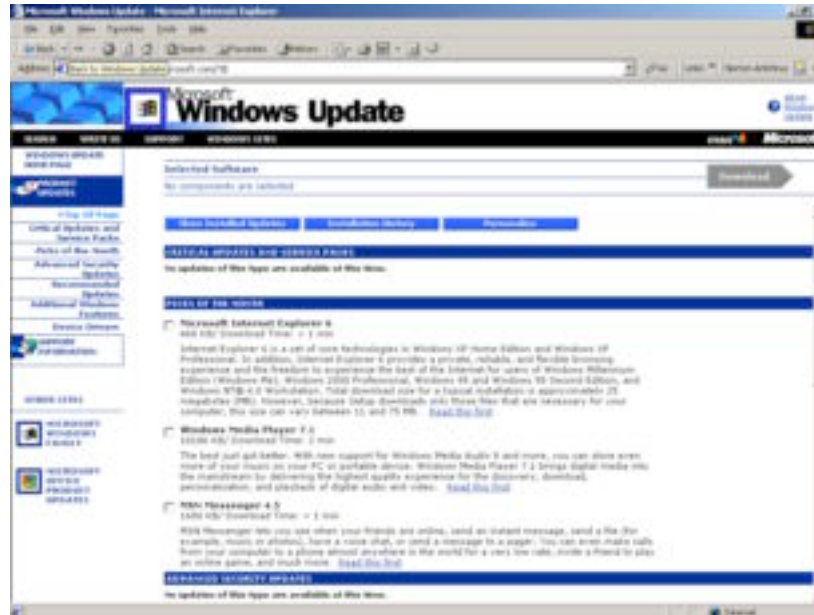
```
[**] [1:1243:2] WEB-IIS ISAPI .ida attempt [**]
[Classification: Web Application Attack] [Priority: 1]
12/13-14:06:30.570996 64.130.103.161:1673 -> 64.225.154.175:80
TCP TTL:127 TOS:0x0 ID:53962 IpLen:20 DgmLen:388 DF
***AP*** Seq: 0xF5FEF2DD Ack: 0x4B13047B Win: 0x10C0 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=can-2000-0071]
[Xref => http://www.whitehats.com/info/IDS552]

[**] [1:1243:2] WEB-IIS ISAPI .ida attempt [**]
[Classification: Web Application Attack] [Priority: 1]
12/13-14:06:30.571022 64.130.103.161:1673 -> 64.225.154.175:80
```

is a screen shot of this rule as configured in the rule set on the Snort sensor:



In Section 12.0 – Patches and Services Packs, Desktop1 is audited to see if has been kept up-to-date with the latest fixes to Windows 2000. Un-patched systems are at significant risk of being targets for hackers. By following the instructions in items 12.1 and 12.2 on Desktop1, one gets the following:



Section 13.0 – Hardened Systems is a section that audits a long list of important security related settings and conditions of Desktop1. Hardening Windows 2000 is vital to having a well-secured system. Below is a report from the Center for Internet Security's Windows 2000 Level One Security Scoring Tool.

Windows 2000 Level One Security Scoring Tool - Host Based - v1.0.0

Computer Name : Desktop1

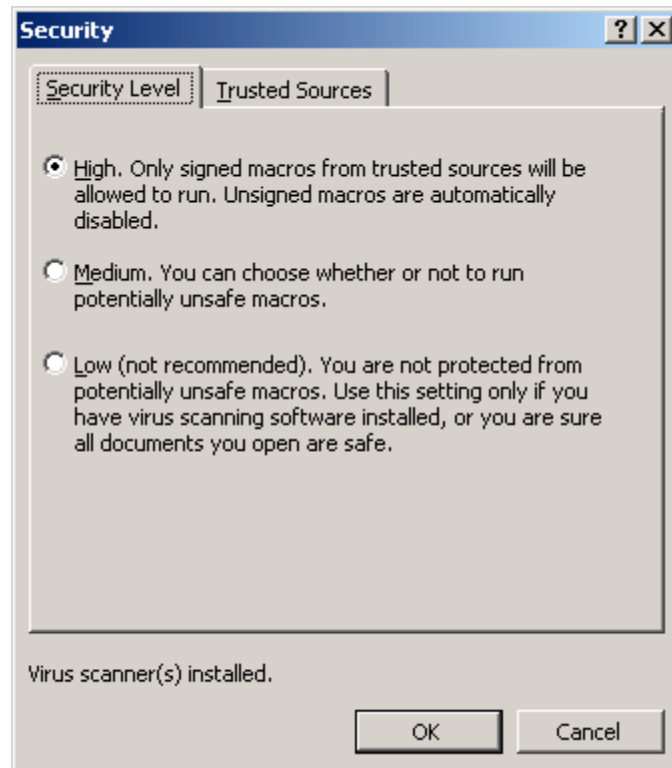
Template : w2k_workstation.inf

Scan Time : 12/12/2001 17:28:45

Description	Value	Score
Service Pack	2	1.667
Hotfixes Needed	2	0
Non-Expiring Passwords	2	0
Policy Mismatches	14	0
Restrict Anonymous	0	0
Security Options Mismatches	11	0
Overall Score		1.7

Description	Mismatches	Total
User Rights	14	49
Group Membership	1	8
Registry Permissions	964	1002
NTFS Permissions	4358	4373
Services	0	58
Password Policy	6	6
Account Lockout Policy	1	1
Event Log Settings	10	10
Audit Policy	7	7
Security Options	11	16

Finally, in Section 14.0 – Macro Protection audits the settings for macro security in Word, Excel, and PowerPoint. This is important because of the many macro viruses that have been launched over the past 3 years. On Desktop1 these settings were set in accordance with the following screen shot:



Here is a summary of the Desktop1 scores from each section:

Section Name	Score
Section 1.0	42
Section 2.0	161
Section 3.0	35
Section 4.0	12
Section 5.0	20
Section 6.0	10
Section 7.0	10
Section 8.0	0
Section 9.0	20
Section 10.0	10
Section 11.0	0
Section 12.0	10
Section 13.0	17
Section 14.0	15
Section 15.0	0
Section 16.0	0
Grand Total	362

3.3 Evaluation of Desktop1 System

By taking the minimum score guidelines listed in Section 2.7 and comparing them to the results in the previous section, the Desktop1 system is “out of spec”. To be specific, the system:

1. Does not have a strong password policy,
2. Has not renamed the built-in Guest account,
3. Does not have non-administrator accounts for regular use,
4. Does not lockout the built-in administrator from network access if the number of failed logins exceeds the threshold set in the local policies,
5. Does not lock non-administrators out from the floppy drive,
6. Does not have any sort of backup, and
7. Needs better Security Options and Security Policies settings.

On a more positive note, the system is well protected from viruses, inappropriate content, worms, and macros. In addition, the firewall, e-mail scanning, and network intrusion detection seem to meet or exceed the minimum standards set forth in Section 2.7.

Here is a list of specific recommendations for bringing this system into compliance:

1. Rename the built-in Guest account. The built-in Administrator account has been renamed, so this is probably a simple oversight. This change should not have any impact on the system since the account is already disabled. This change does not require a lot of time to implement, nor does it require any out of pocket expense.
2. Run passprop.exe. Go to TechNet on Microsoft’s web site and search for “passprop”. Download the resource kit or this specific program, then run it using the /adminlockout option. This is real easy to do, and does not cost any money.
3. Create a non-administrative account for the person(s) that administer the system. Any time one uses the system for non-administrative activities, use the non-administrative accounts. When one needs to “administer” the system, logon with the administrative account, change the system, then logout of the administrative account.
4. Get a copy of floplock.exe from the same resource kit as passprop.exe. Following the installation procedures. This will prevent unauthorized use of the floppy drive.
5. Start performing monthly backups. This is going to require an investment of time and money. Compare and contrast the features of a CDRW versus Taravan/QIC tape drives. It is probably going to cost somewhere between \$300 - \$600 US dollars to obtain adequate hardware for backups of this system.
6. Bring the Account Policies, Local Policies, and Event Log setting into compliance using the following guidelines:
 - a. Enforce password history to remember the last 24 passwords.
 - b. Set the maximum password age to 90 days.
 - c. Set the minimum password age to 1 day.

- d. Set the minimum password length to 12 characters.
 - e. Enable complex password requirements.
 - f. Account lockout duration should be 15 minutes.
 - g. Account lockout threshold should be 3. Three strikes and you're out.
 - h. Account lockout counter should reset after 15 minutes.
 - i. Audit logon/logoff events, success and failure.
 - j. Audit account management, success and failure.
 - k. Audit logon events, success and failure.
 - l. Audit object access failures only.
 - m. Audit policy changes, success and failure.
 - n. Audit privilege use failures only.
 - o. Audit system events, success and failure.
 - p. Limit anonymous access to no access unless explicitly allowed.
 - q. Don't let the system to be shutdown without a logon.
 - r. Enable audit of access to global system objects.
 - s. Enable audit of Backup and Restore privileges.
 - t. Enable clearing of virtual memory on shutdown.
 - u. Enable digital signing of server traffic when possible.
 - v. Always require alt-ctrl-del for logon.
 - w. Enable hiding of last logon name in logon screen.
 - x. Set LAN Manager Authentication level to NTLMV2 only.
 - y. Set the number of cached successful logons to 0.
 - z. Prevent users from installing printer drivers.
 - aa. Restrict CD-ROM access to locally logged-on users only.
 - bb. Restrict floppy access to locally logged-on users only.
 - cc. Enable option to shutdown if security audit events can't be written to the event log.
 - dd. Enable option to lock the workstation on smart card removal.
 - ee. Set unsigned non-driver code option to "warn but allow" during installation.
7. Make changes to the settings for event logs. Use the following guidelines:
- a. Set the application, security, and system logs sizes to 4194240 kilobytes.
 - b. Restrict guest access to the application, security, and system logs.
 - c. Retain the security and system logs for 7 days each.
 - d. Set the retention method for application, security, and system logs to manual.
 - e. Enable shutdown if the security audit log is full.

There are other changes that can be made to improve the security of the system, however the guidelines listed in 6 and 7 above will significantly "harden" it. Keep in mind that the changes in 6 & 7 are time consuming to implement, but they don't cost any money.

In conclusion, the audit shows that the system is well protected at the perimeter of the Internet and against many commonly used attacks and attack vectors. However, the recommendations above will add more layers of defense that will be needed, should an attacker breach any of other defenses. Keep in mind that this system's security is

generally as strong as its weakest link. Based on this audit, a number of weak links need to be addressed.

3.4 Evaluation of the Audit Process

Generally the audit process followed was moderately effective. The overall scoring and comparison with the minimum requirements separated the well-secured areas from the layers of defense that need some improvement, relatively speaking. For a home computer system that has weaknesses, this process and checklist are capable of finding the high priority items that need to be strengthened. However, there are a number of places where problems arose and improvements are needed. In addition, there seem to be a few places where a false sense of security might occur.

Things that were Effective

The checklist, tools and methodologies for evaluating the firewall, virus scanning software, network based intrusion detection, hardened OS, patches and service packs are effective at determining the state of these layers of defense. Each test item is relatively simple to perform, and it was easy to know how to score the system in these areas. In addition, it was fairly easy to collect the results of these tests in the form of screen shots, logs, and/or general text output.

Also, given the guidelines in Section 2.7 it is easy to see where the system is “out of spec”. There are issues with individual elements of these guidelines, but assuming these are improved, the minimum scores provide a clear indication of what needs attention.

Problems Encountered

Many of the questions in Section 1.0 of the checklist are subjective, and most of the possible answers are difficult to record. For example, people that aren’t aware of security issues on their home computer are likely to give all sorts of answers to the question, “What actions do you take when you walk away from your computer?” This leads to difficulty in figuring out how to score the item.

In Section 6.0 – Content Filtering, steps are laid out to determine if the ad blocking features were working or not. The testing steps for this did not yield consistent results. Part of the problem is the way many web sites do “ad rotation” and/or modify the behavior of the home page based on the number of visits. By jumping around to various popular web sites that derive most of their revenues from advertising, one can determine if the ad blocking is working or not. This type of test does require loading several home pages before one knows for sure.

Needed Improvements

The questions in Section 1.0 should be redesigned into a meaningful scaling method, such as a Likert Scale²⁵. This would improve the accuracy of measuring the behavior and awareness of the user toward computer security.

Item 2.4 needs a different means to measure the relative security of applications configured to pass through the personal firewall. It is not clear that the current approach accomplishes this goal. The idea is to test to see if the personal firewall is being configured in a manner consistent with the principal of least privilege.

Test item 6.3 could use a program that simply tries HTTP into a known, but undisclosed, adult content home page, then simply returns whether access was obtained or blocked. This way the auditor and/or anyone watching over the shoulder of the auditor would not have to risk seeing something he or she does not want to see.

False Indicators

The minimum score for Section 3.0 – Anti-virus Software is too low. There are six important audit items in this Section. If a system meets the requirement for two or three, then it is possible one might think the system is adequately protected from viruses. If you've never updated the virus definitions files since installation, then scanning and auto-protection is not worth much.

The program used in Section 11.0, audituf.exe, can lead one to believe that there isn't any unused software on the system. Because the virus scanning software is running every week or so, all the executable programs are going to have a last accessed date within the last 30 days. The audituf.exe program checks the last accessed date on all executables to see if any have not been accessed in the last 90 days. If a small percentage of the files have not been accessed within the last 90 days, then audituf.exe gives a minimum score of 10. This could be completely misleading. The only thing that audituf.exe can determine with accuracy is whether the OS2 and POSIX subsystem files have been removed.

References

1. Hazari, Sunil, Ph.D. "Developing Good Security Habits." Secure Online Behavior. 28 May 2001. SecurityFocus™ .
[URL:http://www.securityfocus.com/infocus/1195](http://www.securityfocus.com/infocus/1195) (7 November 2001).
2. Hazari, Sunil, Ph.D. "Part II: Secure E-Mail Behavior." Secure Online Behavior. 20 June 2001. SecurityFocus™ . [URL:http://www.securityfocus.com/infocus/1196](http://www.securityfocus.com/infocus/1196) (7 November 2001).
3. Hazari, Sunil, Ph.D. "Part Three: Using the World Wide Web." Secure Online Behavior. 2 July 2001. SecurityFocus™ .
[URL:http://www.securityfocus.com/infocus/1197](http://www.securityfocus.com/infocus/1197) (7 November 2001).
4. Anderson, Jared M. Ethics in Grade Schools. 20 November 1998.
[URL:http://courses.cs.vt.edu/professionalism/Schools/Anderson/](http://courses.cs.vt.edu/professionalism/Schools/Anderson/) (8 November 2001).
5. Anderson, Jared M. "Purpose & Objectives." Ethics in Grade Schools. 20 November 1998.
[URL:http://courses.cs.vt.edu/professionalism/Schools/Anderson/purpose.html](http://courses.cs.vt.edu/professionalism/Schools/Anderson/purpose.html) (8 November 2001).
6. Anderson, Jared M. "RE: Questions about Ethics in Grade Schools." E-mail to Scott L. Reeder. 13 November 2001.
7. Wood, Charles Cresson. "The Human Firewall Manifesto." The Human Firewall. October 2001. URL:<http://www.humanfirewall.com/rhfw.htm> (13 November 2001).
8. "Top 10 most common info security mistakes made by individuals." The Human Firewall. October 2001. [URL:http://www.humanfirewall.com/rhfw.htm](http://www.humanfirewall.com/rhfw.htm) (13 November 2001).
9. Horowitz, Alan S. "Top 10 Security Mistakes." Computerworld. 9 July 2001.
[URL:http://www.computerworld.com/cwi/story/0,1199,NAV47_STO61986,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO61986,00.html) (13 November 2001).

10. "Statement on Individual Responsibilities in Shared Computing Environments at Carnegie Mellon University." Faculty Handbook. 15 September 1987. Carnegie-Mellon University.
URL:http://gollum.mac.cc.cmu.edu/univ_policy/documents/ShareComp.html (14 November 2001).
11. "Carnegie Mellon University Computing and Information Resources Code of Ethics." Student Handbook. Carnegie-Mellon University.
URL:http://gollum.mac.cc.cmu.edu/univ_policy/documents/CompEthics.html (14 November 2001).
12. "Policy 2020: Policy on Protecting Electronic Access Privileges." Policy and Procedures. 8 December 1998. Virginia Polytechnic Institute and State University. URL:<http://www.vt.edu/admin/policies/1000/2020.html> (8 November 2001).
13. "Acceptable Use of Information Systems at Virginia Tech." 16 June 2000. Virginia Polytechnic Institute and State University.
URL:<http://www.vt.edu/admin/policies/acceptuseguide.html> (8 November 2001).
14. Nahar, Sushilkumar. "Securing the Broadband Network." SANS Reading Room. 9 August 2001.
URL:<http://www.sans.org/infosecFAQ/homeoffice/broadband.htm> (10 November 2001).
15. Lie, Hans. "More Secure @home Using Linux." SANS Reading Room. 15 September 2001.
URL:http://www.sans.org/infosecFAQ/homeoffice/more_sec.htm (10 November 2001).
16. Dean, Ron. "The Importance of Social Engineering for the Home Internet User." SANS Reading Room. 16 July 2001.
URL:<http://www.sans.org/infosecFAQ/homeoffice/social.htm> (10 November 2001).
17. Heyn, Frederick M. "Batten Down the Net Hatches: Making Your 24x7 Home Access to the Internet as Secure as Possible." SANS Reading Room. 9 May 2001. URL:<http://www.sans.org/infosecFAQ/homeoffice/hatches.htm> (10 November 2001).
18. Carter, Bryan Carter. "Security Concerns About Multimedia Technologies." SANS Reading Room. 22 November 2000.
URL:<http://www.sans.org/infosecFAQ/homeoffice/concerns.htm> (10 November 2001).

19. "Home Network Security." CERT® Coordination Center. 6 August 2001. Carnegie Mellon University.
[URL:http://www.cert.org/tech_tips/home_networks.html](http://www.cert.org/tech_tips/home_networks.html) (8 November 2001).
20. DeBonis, Marc. "Making Microsoft NT 4.0 Server a secure operating system." Version v991101.1133. November 1999.
[URL:http://bunbun.ais.vt.edu/work/securing_nt.html](http://bunbun.ais.vt.edu/work/securing_nt.html) (8 November 2001).
21. The SANS Institute. SANS Securing Windows 2000 Step-by-Step Guide. Version 1.5. Ed. Jeff Shawgo. 1 July 2001.
22. Elky, Steve. "Automated Auditing in a Windows 2000 Environment." SANS Institute Security Digests. 13 August 2001. SANS Institute.
[URL:http://www.sans.org/newlook/digests/auto_audit.htm](http://www.sans.org/newlook/digests/auto_audit.htm) (3 December 2001).
23. Haney, Julie M. "Guide to Securing Microsoft Windows 2000® Group Policy: Security Configuration Tool Set." Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC). Version 1.0. 17 May 2001. National Security Agency, United States of America.
[URL:http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf](http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf). (3 December 2001).
24. The Center for Internet Security. Level One Benchmark Windows 2000 Operating System. Ed. Jeff Shawgo. November 2001.
[URL:http://www.cisecurity.org/bench_win2000.html](http://www.cisecurity.org/bench_win2000.html) (3 December 2001).
25. Davis, Duane, and Cosenza, Robert M. Business Research for Decision Making. Ed. John B. Mchugh. Boston: PWS-Kent Publishing Company, 1985. 170-191.

Appendix A – Source Code for auditvap.exe

Written for Microsoft Visual Studio VC/C++

```
#include <stdio.h>
```

```
void main( void )  
{
```

```
    FILE *stream;  
    char signature[] = "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-  
ANTIVIRUS-TEST-FILE!$H+H*";  
    char *tfilename = NULL;  
    char filename[255] = "\0";
```

```
    try  
    {  
        tfilename = tmpnam(NULL);  
        sprintf(filename,"%scom\0",tfilename);  
  
        stream = fopen(filename,"w");  
        fwrite(signature,sizeof(signature),sizeof(signature),stream);  
  
        fclose(stream);  
        remove(filename);  
    }  
    catch(...)  
    {  
        perror("auditvap");  
    }  
}
```

Appendix B – Source Code for audituf.exe

Written for Microsoft Visual Studio VC/C++

```
#include <windows.h>
#include <stdio.h>

DWORD dwTotalEXEFiles = 0L;
DWORD dwUnUsedEXEFiles = 0L;
DWORD dwOS2PosixFiles = 0L;

FILETIME ft3MonthsAgo;

float ScoreOS2AndPosix(void)
{
    char *strFileList [] = {
        "os2.exe\0",
        "os2srv.exe\0",
        "os2ss.exe\0",
        "posix.exe\0",
        "psxdll.dll\0",
        "psxss.exe\0",
        NULL
    };

    DWORD dwCount = 0L;
    DWORD dwFilesFound = 0L;
    HANDLE hFind = NULL;
    WIN32_FIND_DATA fData;

    char strFind[MAX_PATH]="\0";
    char strSystemPath[MAX_PATH]="\0";

    GetSystemDirectory(strSystemPath,MAX_PATH);

    while(strFileList[dwCount] != NULL)
    {
        memset(strFind,0,MAX_PATH);
        sprintf(strFind,"%s\\%s\0",strSystemPath,strFileList[dwCount]);

        hFind = FindFirstFile(strFind,&fData);
        if(hFind != INVALID_HANDLE_VALUE)
        {
            FindClose(hFind);
            dwOS2PosixFiles++;
        }
        dwCount++;
    }

    if(dwOS2PosixFiles == 0)
        return (float)5.0;
    else
        return (float)0.0;
}

void ProcessSubDir(const char *strDir)
{
    HANDLE hFind = NULL;
    WIN32_FIND_DATA fData;
```

```

char strFind[MAX_PATH]="\0";
char strNewPath[MAX_PATH]="\0";

sprintf(strFind,"%s\\*.\\0",strDir);

hFind = FindFirstFile(strFind,&fData);
if(hFind != INVALID_HANDLE_VALUE)
{

    if(fData.dwFileAttributes | FILE_ATTRIBUTE_DIRECTORY)
    {
        if(strcmp(fData.cFileName,".\0") && strcmp(fData.cFileName,"..\0"))
        {
            sprintf(strNewPath,"%s\\%s\0",strDir,fData.cFileName);
            ProcessSubDir(strNewPath);
        }
        memset(strNewPath,0,MAX_PATH);
    }

    while(FindNextFile(hFind,&fData))
    {
        if(fData.dwFileAttributes | FILE_ATTRIBUTE_DIRECTORY)
        {
            if(strcmp(fData.cFileName,".\0") && strcmp(fData.cFileName,"..\0"))
            {
                sprintf(strNewPath,"%s\\%s\0",strDir,fData.cFileName);
                ProcessSubDir(strNewPath);
            }
        }
        memset(strNewPath,0,MAX_PATH);
    }
    FindClose(hFind);
}

memset(strFind,0,MAX_PATH);
sprintf(strFind,"%s\\*.exe\0",strDir);

hFind = FindFirstFile(strFind,&fData);
if(hFind != INVALID_HANDLE_VALUE)
{
    dwTotalEXEFiles++;
    if(CompareFileTime(&fData.ftLastAccessTime,&ft3MonthsAgo)!=1)
        dwUnusedEXEFiles++;

    while(FindNextFile(hFind,&fData))
    {
        dwTotalEXEFiles++;
        if(CompareFileTime(&fData.ftLastAccessTime,&ft3MonthsAgo)!=1)
            dwUnusedEXEFiles++;
    }
    FindClose(hFind);
}

}

void ProcessLogicalDrive(const char *strDir)
{

    HANDLE hFind = NULL;
    WIN32_FIND_DATA fData;

    char strFind[MAX_PATH]="\0";
    char strNewPath[MAX_PATH]="\0";

```



```

sprintf(strFind,"%s*.\\0",strDir);

hFind = FindFirstFile(strFind,&fData);
if(hFind != INVALID_HANDLE_VALUE)
{

    if(fData.dwFileAttributes | FILE_ATTRIBUTE_DIRECTORY)
    {
        if(strcmp(fData.cFileName,".\\0") && strcmp(fData.cFileName,"..\\0"))
        {
            sprintf(strNewPath,"%s%s\\0",strDir,fData.cFileName);
            ProcessSubDir(strNewPath);
        }
        memset(strNewPath,0,MAX_PATH);
    }

    while(FindNextFile(hFind,&fData))
    {
        if(fData.dwFileAttributes | FILE_ATTRIBUTE_DIRECTORY)
        {
            if(strcmp(fData.cFileName,".\\0") && strcmp(fData.cFileName,"..\\0"))
            {
                sprintf(strNewPath,"%s%s\\0",strDir,fData.cFileName);
                ProcessSubDir(strNewPath);
            }
        }
        memset(strNewPath,0,MAX_PATH);
    }
    FindClose(hFind);
}

memset(strFind,0,MAX_PATH);
sprintf(strFind,"%s*.exe\\0",strDir);

hFind = FindFirstFile(strFind,&fData);
if(hFind != INVALID_HANDLE_VALUE)
{
    dwTotalEXEFiles++;
    if(CompareFileTime(&fData.ftLastAccessTime,&ft3MonthsAgo)!=1)
    {
        dwUnusedEXEFiles++;
        // printf("\t\t%s\n",fData.cFileName);
    }

    while(FindNextFile(hFind,&fData))
    {
        dwTotalEXEFiles++;
        if(CompareFileTime(&fData.ftLastAccessTime,&ft3MonthsAgo)!=1)
        {
            dwUnusedEXEFiles++;
            // printf("\t\t%s\n",fData.cFileName);
        }
    }
    FindClose(hFind);
}

}

int main(void/*int argc, char* argv[]*/)
{
    char *logicaldrive = NULL;
    char delimiter [] = " ";
    char logicaldriveslist[MAX_PATH] = "\\0";
    DWORD dwlistsize = 0L;

```

```

DWORD dwcharcount = 0L;
float dwScore = 0.0;
float dwRatio = 0.0;
char *p = NULL;
SYSTEMTIME stCurrentTime;

```

```

try
{

```

```

    GetSystemTime(&stCurrentTime);

    if(stCurrentTime.wMonth <= 3)
    {
        switch (stCurrentTime.wMonth)
        {
            case 2:
                stCurrentTime.wYear = stCurrentTime.wYear - 1;
                stCurrentTime.wMonth = 12;
                break;

            case 1:
                stCurrentTime.wYear = stCurrentTime.wYear - 1;
                stCurrentTime.wMonth = 11;
                break;

            case 0:
                stCurrentTime.wYear = stCurrentTime.wYear - 1;
                stCurrentTime.wMonth = 10;
                break;

            default:
                stCurrentTime.wYear = stCurrentTime.wYear - 1;
                stCurrentTime.wMonth = 9;
                break;
        }
    }
    else stCurrentTime.wMonth = stCurrentTime.wMonth - 3;

    SystemTimeToFileTime(&stCurrentTime,&ft3MonthsAgo);

    dwlistsize = GetLogicalDriveStrings(MAX_PATH,logicaldriveslist);
    if(dwlistsize!=0 && dwlistsize < MAX_PATH)
    {
        //replace intra-string nulls with whitespace so we can use strtok() with
        //whitespace as a delimiter
        while(dwcharcount <= dwlistsize)
        {
            p = &logicaldriveslist[dwcharcount];
            if(p[0] == NULL)
            {
                p[0] = ' ';
            }
            dwcharcount++;
        }

        //now parse for individual drives
        logicaldrive = strtok(logicaldriveslist,delimiter);

        while(logicaldrive!=NULL)
        {
            if(GetDriveType(logicaldrive) == DRIVE_FIXED)
            {
                //now we have a fixed logical drive letter
                printf("Processing drive %s\n",logicaldrive);
                ProcessLogicalDrive(logicaldrive);
            }
        }
    }
}

```

```

        }
        logicaldrive = strtok(NULL,delimiter);
    }

}

printf("Total EXE files = %d\n",dwTotalEXEFiles);
printf("Total Un-used EXE files = %d\n",dwUnUsedEXEFiles);

dwRatio = (float)dwUnUsedEXEFiles / (float)dwTotalEXEFiles;
dwScore = ((float)10.0 * ((float)1.0 - dwRatio)) + ScoreOS2AndPosix();

printf("Total OS2 or Posix files = %d\n",dwOS2PosixFiles);

printf("Score = %1.0f\n",dwScore);

}
catch(...)
{
    perror("audituf");
}

return 0;
}

```