



# 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/gsna>

***Special Permission Project:***  
**Mobile Computing Self Assessment  
for Non-technical Business Users**

**By Michael Patrick Hagerty, GSEC**

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

## Table of Contents

<b>1</b>	<b><i>Research</i></b>	<b>5</b>
1.1	<b>Background</b>	<b>5</b>
1.2	<b>Scope</b>	<b>7</b>
1.3	<b>Assumptions</b>	<b>7</b>
1.4	<b>Risks and Associated Costs</b>	<b>8</b>
1.4.1	Outright loss of laptop	8
1.4.2	Loss of data through disk/system failure or deletion	9
1.4.3	Loss of system integrity through infection by viruses	10
1.4.4	Loss of security of data through unauthorized access	10
1.4.5	Loss through propagation of problems to other systems	11
1.4.6	Loss through financial liability accrued by consultant	12
1.4.7	Loss through degradation of consultant/company image	13
1.5	<b>Mitigation of Above Risks</b>	<b>13</b>
1.5.1	Outright loss of laptop	13
1.5.2	Loss of data through disk/system failure or deletion	13
1.5.3	Loss of system integrity through infection by viruses	13
1.5.4	Loss of security of data through unauthorized access	14
1.5.5	Loss through propagation of problems to other systems	14
1.5.6	Loss through financial liability accrued by consultant	14
1.5.7	Loss through degradation of consultant/company image	15
1.6	<b>Mapping of Mitigations to Company Policy</b>	<b>15</b>
1.7	<b>Base System Configuration</b>	<b>15</b>
1.8	<b>Assessment Tools</b>	<b>16</b>
<b>2</b>	<b><i>Assessment/Audit Process</i></b>	<b>17</b>
2.1	<b>Physical Security</b>	<b>17</b>
2.1.1	Laptop Bag Identification	17
2.1.2	Asset Identification	17
2.1.3	Physical Lockdown	18
2.2	<b>Boot Process</b>	<b>18</b>
2.2.1	Boot Password	18
2.2.2	Boot Devices	19
2.3	<b>System Password</b>	<b>19</b>
2.4	<b>Antivirus Protection Status</b>	<b>20</b>
2.5	<b>Firewall Status</b>	<b>22</b>
2.6	<b>Lotus Notes Protection</b>	<b>23</b>

2.6.1	Notes Passwords.....	23
2.6.2	Notes Email Database Encryption.....	23
<b>2.7</b>	<b>Operating System &amp; MS-Office Status .....</b>	<b>24</b>
2.7.1	Windows 2000 Update.....	24
2.7.2	Office 2000 Update .....	24
<b>2.8</b>	<b>Microsoft Baseline Security Scan .....</b>	<b>24</b>
<b>2.9</b>	<b>Additional Email Client.....</b>	<b>25</b>
<b>2.10</b>	<b>System/File Backup .....</b>	<b>26</b>
<b>2.11</b>	<b>ISP Dialer .....</b>	<b>27</b>
<b>2.12</b>	<b>User Installed Applications .....</b>	<b>27</b>
<b>3</b>	<b><i>An Application of the Assessment Process.....</i></b>	<b>29</b>
<b>3.1</b>	<b>Physical Security .....</b>	<b>29</b>
3.1.1	Laptop Bag Identification .....	29
3.1.2	Asset Identification .....	29
3.1.3	Physical Lockdown .....	29
<b>3.2</b>	<b>Boot Process.....</b>	<b>30</b>
3.2.1	Boot Password.....	30
3.2.2	Boot Devices.....	31
<b>3.3</b>	<b>System Password.....</b>	<b>31</b>
<b>3.4</b>	<b>Antivirus Protection Status.....</b>	<b>31</b>
<b>3.5</b>	<b>Firewall Status.....</b>	<b>34</b>
<b>4</b>	<b><i>Security Implications.....</i></b>	<b>34</b>
<b>4.1</b>	<b>Lotus Notes Protection.....</b>	<b>35</b>
4.1.1	Notes Passwords.....	35
4.1.2	Notes Email Database Encryption.....	35
<b>4.2</b>	<b>Operating System &amp; MS-Office Status .....</b>	<b>36</b>
4.2.1	Windows 2000 Update.....	36
4.2.2	Office 2000 Update .....	36
<b>4.3</b>	<b>Microsoft Baseline Security Scan .....</b>	<b>37</b>
<b>4.4</b>	<b>Additional Email Client.....</b>	<b>40</b>
<b>4.5</b>	<b>System/File Backup .....</b>	<b>41</b>
<b>4.6</b>	<b>ISP Dialer .....</b>	<b>42</b>
<b>4.7</b>	<b>User Installed Applications .....</b>	<b>42</b>
<b>4.8</b>	<b>Is the Laptop Securable? .....</b>	<b>47</b>

4.9	Is the System Auditable? .....	47
<b>5</b>	<b><i>Follow Up to the Self-Assessment</i>.....</b>	<b>49</b>
5.1	Summary.....	49
5.2	Identified Problems .....	49
5.3	Risk .....	50
5.4	Ignored Issues.....	51
5.5	Review of the Process .....	51
5.6	Conclusion.....	51
	<b><i>Appendix A - Use of Electronic Communication Systems and Media Management Policy (amended for Consulting Group)</i>.....</b>	<b>53</b>
	<b><i>Appendix B – ZoneAlarm Log</i>.....</b>	<b>58</b>
	<b><i>Appendix C -- Inadequately Addressed Problems</i>.....</b>	<b>73</b>
C.1	User Warning on Impending Disk Failure.....	73
C.2	Encrypted Disks .....	74
C.3	Advertisement/Popup Filter.....	74
	<b><i>Bibliography</i>.....</b>	<b>75</b>

## Table of Figures

Evidence 1 - Laptop Case Identification.....	29
Evidence 2 - Laptop Lockdown Cable Use .....	30
Evidence 3 - Successful Boot Password.....	30
Evidence 4 - Photograph of system manager screen.....	31
Evidence 5 - Response from Password.exe .....	31
Evidence 6 - Antivirus Configuration .....	32
Evidence 7 - Quarantined Attachments .....	33
Evidence 8 - Indication of intercepted virus test file .....	34
Evidence 9 - Port table from ShieldsUP! Probe My Ports.....	35
Evidence 10 - Windows Update Capture.....	36
Evidence 11 - Office 2000 Update Report.....	37
Evidence 12 - MBSA Report.....	38
Evidence 13 - Disabled Rich Text (HTML) Messaging.....	40
Evidence 14 - Intercepted virus .....	41
Evidence 15 - Example Registration Screens .....	43

# 1 Research

I am *developing a checklist to assess* a consulting company user's laptop, an IBM 600X ThinkPad running Windows 2000 as its operating system, for compliance with the company's published policy. The company's policy covers all computing and communications equipment, media and systems, but does not provide checklists, or a list of tools and/or practices to facilitate, measure or ensure compliance. This document presents a refinement and implementation process for the policy as it applies to a class of equipment used extensively by employees of the company's consulting division, namely laptops.

## 1.1 Background

Each consultant is provided as part of his/her "kit" a laptop preloaded with the "standard" operating system, a suite of software tools, COTS (commercial off the shelf) applications, and access to a set of proprietary data files. Included in their initial orientation is a brief discussion of the company's policy on the use of computing and communications equipment, included as Appendix A, and the consequences of failing to comply with the policy, although no explicit training is provided at that time on how to maintain the level of security engineered in the laptop's original image.

A significant number of the consultants will be expected to spend the majority of their time on distant travel assignments. In these cases, the policy's Section 4.2 tight constraints on personal use are relaxed somewhat; consultants are not expected to carry along an additional, personal, computer for their use while staying in hotels company-provided apartments on long-term assignments. This relaxation, complicated by the consultants' potentially infrequent visits to a company facility and their ability to both install additional software and modify pre-existing settings, creates an opportunity for consultants to cause their laptops to drift away from the level of security that could be maintained at the company's facilities.

Consultants use these laptops at home, in airports and on planes, in hotels and while connected to client networks. A host of company and client confidential and/or proprietary information and applications finds a home on these machines, creating a considerable liability for the company in the event of compromise or loss. In the past, laptops have been stolen, lost, infected beyond the ability to recover data, run over and destroyed or simply stop functioning due to disk failure. In many cases, the value of the information contained on these laptops greatly exceeded the cost of the laptop itself

Within the company's physical reach, machines (specifically, the data and applications on the machines) are protected via firewalls, with active virus scanning and full backup of all company provided applications and user created data. However, once free of the company's ability to manage the systems, security weakens. Furthermore, the company has provided neither tools nor guidance to the consultants on how they might maintain

consistent security levels on their laptops. In one instance, a consultant went for almost two years without backing up his laptop before it was stolen while it was sitting on a desk unattended and unsecured at a client site. A vast amount of work product, as well as all of the consultant's personal files and correspondence vanished without a trace. The consultant's hope was that the thief would reformat the disk to eliminate evidence before selling it and thereby limit potential compromise of company/client proprietary and personal information.

The experience described above is not unique and indicates that problems in the field can have a direct effect on the Company's products. However, those inside the Company firewall may not have the perspective to appreciate the problems encountered in the field and remedies that work inside the company firewall may not be helpful out in the field.

As mentioned above, tools are not provided to permit the consultant to backup the laptop files although the initial briefing makes it clear that the consultant is responsible for the loss of any work product on the laptop. A technician at the office will, upon returning the laptop for repair, reformat the disk and image it with the then standard image. Unfortunately, this process ignores any user or client data that may have been added. This makes sending the laptop back to the office for re-imaging an undesirable option for most consultants. Any software they may have installed on the system to assist them on a particular assignment would be wiped as would any personal applications. Many consultants periodically perform ad hoc backups of specific data directories, but this is far from universal, rarely systematic and usually ignores whatever else they may have on their laptops.

A separate problem exists in that the consultants may not have updated their antivirus protection and system patches. They may have misconfigured the utility which, coupled with lax computing practices, may lead to system corruption, data loss or even create a situation in which the company's reputation is harmed when a consultant's laptop begins propagating a virus or worm to clients, etc. Despite cautions offered, many consultants, will connect their laptops to home networks where children, skilled beyond their wisdom, may be engaging in unsafe computing practices adversely affecting company property.

Despite having a published policy, the company faces a considerable liability which in-house security technology, process and procedures has not addressed save through repeated messages pointing to the policy and admonitions to practice "safe hex" out in the field. Although the company's lawyers may be satisfied with such poster notifications, those responsible for the client and company information on these machines are justified in asking for evidence of actual compliance.

## 1.2 Scope

The scope of this paper is limited to providing an audit checklist, essentially a self-assessment, to determine the current state of processes, practices, tools and configuration of a consultant's laptop relative to the level recommended to protect the company's assets outside of the company's offices. Because of the requirement for administrator privilege to install additional software, patches or updates on Windows 2000 in the field, the consultant has an administrator account on his/her laptop and, in the context of this assignment's guidelines, is the system administrator.

This paper specifically does not address the configuration of the initial image installed on the laptop.

The consultants who do not feel competent to perform the assessment may return the laptop to a local office where a system administrator will perform the assessment.

Consistent with the course text, the audit/assessment is not to be viewed as a cop's interrogation, looking for wrongdoing. It is an effort to assist the consultant in protecting the work products into which s/he has poured much labor and in maintaining their image as both competent and professional, as well as protect the assets of the company.

## 1.3 Assumptions

This paper assumes the consultant understands the policy, will not engage in the practices prohibited in Section 4 of the policy and is aware that the company can, at any time, require the surrender of any and all property provided by the company to verify compliance with the terms of the policy.

The initial image on the laptop was engineered by competent systems engineers based on the latest security best practices and recommendations from Microsoft, SANS, the NSA and other organizations, e.g., Microsoft's "Windows 2000 Professional Configuration."<sup>1</sup>

The consultant is a moderately knowledgeable computer user who happens to have administrator privilege to this one machine, but is not a security expert. While s/he can install, run and configure applications, this paper does not anticipate the consultant will be modifying the registry directly.

The consultant has online access through which s/he can download updates and patches.

---

<sup>1</sup> "Windows 2000 Professional Configuration," **Windows 2000 Professional Baseline Security Checklist**, Microsoft Corporation,  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2kproclasp>



Any tools not included in the image created on 9/1/2001 are provided on a CD to accompany this document.

## 1.4 Risks and Associated Costs

The risk to the company attributable to a consultant's laptop can be divided into seven areas of "loss" each of which presents costs to the company.

1. Outright loss of the device with subsequent compromise of information
2. Loss of data through unrecoverable disk or system failure or deletion
3. Loss of system integrity through infection by viruses
4. Loss of security of data through unauthorized access
5. Loss through propagation of problems to other systems
6. Loss through financial liability accrued by consultant
7. Loss through degradation of consultant/company image

The Company policy addresses each of the above, albeit in indirect fashion. This section defines the risks while Section 1.4 will discuss the means of mitigating these risks. Where specifically broken out in the **2002 CSI/FBI Computer Crime and Security Survey**<sup>2</sup>, industry-wide loss in projected dollars is also provided.

### 1.4.1 Outright loss of laptop

As the target of this audit is a fairly portable, freely accessible, and easily stolen device, the most obvious risk is total loss through theft or being misplaced by the user, with the possible compromise of all sensitive information contained thereon. Although the CSI/FBI study indicates that this happens often, the means for controlling this loss, e.g., vigilance, easy identification and physical control, are readily understood. Most often the loss occurs because the consultant left the laptop or the case containing the laptop in plain sight, unattended and not secured to anything sufficiently massive to prevent someone from picking the laptop up and walking away with it. Loss can also occur during travel when the consultant is separated from his/her bag, e.g., at the airport checkpoints, or when a laptop bag is stuffed into the trunk of a cab or left at curbside.

Laptop theft is a huge problem, according to security industry and insurance company statistics. Safeware (www.safeware.com), an Ohio-based insurance firm specializing in PC policies, reports that nearly 320,000 laptops valued at \$800 million were stolen in 1999, a 5 percent increase over the previous year.<sup>3</sup>

<sup>2</sup> **2002 CSI/FBI Computer Crime and Security Survey**, Volume VIII, Number 1, Spring 2002, Computer Security Institute

<sup>3</sup> "Locking Down the Laptop," Paul Korzeniowski, **Information Security**, February 2001, [http://www.infosecuritymag.com/articles/february01/features\\_laptop\\_security.shtml](http://www.infosecuritymag.com/articles/february01/features_laptop_security.shtml)

In all instances, once the laptop is gone, it must be assumed that an unauthorized person is reading all information on the laptop. Boot passwords, login passwords and all of the operating system security are essentially useless once an individual has unrestricted physical access to the device for as long as they want. JSI Inc.'s website offers a detailed step-by-step process to recover the admin password to an NT/2000 system<sup>4</sup> noting, **“There is no security without physical security!”**

The cost to the Company of outright loss is

- Cost of the laptop;
- Potential loss of confidential and/or proprietary information to competitors and any future business this might affect;
- Downtime incurred by the consultant while a replacement system is configured, imaged and shipped out; and
- Cost to recover any work products in progress at the time of loss.

Industry-wide, laptop theft is reported by 145 of the 503 respondents in the CSI/FBI Survey. This is the second most commonly reported loss, amounting to \$11.6M.

### 1.4.2 Loss of data through disk/system failure or deletion

Disk drives will fail eventually; it is their defined end-of-life condition, although there are times when some advance warning is available. When information is lost through disk/system failure or inadvertent deletion, the question “Is this information available elsewhere and can be restored quickly and/or economically?” arises. In other words, “Do you have a backup?” I am often reminded that far too few people follow the maxim, “Backup like voting in Chicago: early and often!” Although most consultants understand the concept, many simply fail to back up their critical data because they do not have the tools to accomplish the task in the field. History has shown that telling a consultant to back up their critical data without providing them the means to accomplish that task and the confidence to perform it is futile.

Furthermore, relying upon a backup scheme without testing the system's ability to actually recover data previously backed up has led to rude surprises on more than one occasion. For example, a version of the Zenith/DOS restore program was incapable of restoring any file backed up on the 10<sup>th</sup> day of any month or any day of the 10<sup>th</sup> month. This flaw was only discovered upon attempting to restore a file that had backed up on the 10<sup>th</sup> day of the 10<sup>th</sup> month and, as most former DOS users are aware, a file had to be restored with the same numbered version of the restore program as that of the backup program that originally backed it up.

---

<sup>4</sup> JSI, INC. - Your Windows NT; / Windows 2000; Resource, “0554 » Lost your Administrator password and need the ultimate hack?” <http://www.jsiinc.com/subb/tip0500/rh0554.htm>

Included in this category are losses due to errors of judgment on the part of the consultant, including dropping the laptop, subjecting it to adverse conditions or, as has actually happened, driving over the laptop.

The cost to the company of disk/system failure or file deletion is

- Cost of replacing the failed disk and/or system with a standard image disk or system;
- Downtime incurred by the consultant while a replacement system is configured, imaged and shipped out; and
- Cost to recover any work products in progress at the time of loss.

### **1.4.3 Loss of system integrity through infection by viruses**

Computer viruses can corrupt and/or delete data and/or applications on laptops. The vectors for viruses to make their way into Company laptops is through infected email or attachments thereto, infected files that are downloaded or installed on the machine or through open shares or back doors providing access to the machine's file system. Originally, only files with the .exe or .com extensions were capable of infecting Windows systems, but with the advent of powerful macro languages and their inclusion in a wide range of products, e.g., spreadsheets, PowerPoint presentations and Word documents, as well as the system's ability execute a file that has been re-labeled with an innocuous extension, files of all types are potential vectors.

A virus can cause both immediate loss of data and/or application functionality as well as a kind of slow creeping corruption that manifests itself by the machine appearing slower over time and/or files begin disappearing. The cost to the Company of loss resulting from viral infection is

- Cost of disinfecting (if possible) the system or
- Cost of re-imaging the system with the standard image and work products;
- Downtime incurred by the consultant while the system is cleansed of the worm; virus or trojan, or a replacement system is configured, imaged and shipped out; and
- Cost to recover any work products in progress at the time of loss.

The CSI/FBI Survey reports that viruses account for an annual loss to industry of approximately \$50M, with 188 (the highest) of those surveyed quantifying attacks. I believe the percentage of respondents reporting in this category to be low, perhaps only those who had faced a system-wide attack had responded.

### **1.4.4 Loss of security of data through unauthorized access**

The security of company and client data can be compromised through unauthorized access by several means: An unlocked, unattended laptop invites access by those passing by, what lawyers call an "attractive nuisance" and, assuming that the individual accessing

the machine has not compromised the system by introducing malware, i.e., viruses, worms or trojans, the loss would be limited to the disclosure of potentially sensitive and/or proprietary company or client data. This loss could affect both current and future engagements and relationships, as well as negatively color the image of both the company and the individual consultant with regard to protecting the assets of clients.

If the system has been compromised by the introduction of a back door application, the loss of information may have been ongoing for some period of time. In this case, it may be impossible to determine what information was accessed; by whom and to what purpose the access portal was introduced.

One area, also in this category, which is seemingly overlooked by many companies, is unauthorized access through inadvertent disclosure. Motorola, having lost a trade secret protection case as a result of their inability to demonstrate diligence in protecting trade secrets, later produced an internal training program to raise awareness and prevent future losses. The training program taught its employees to assume the competition was all around them in public, e.g., when sitting on an airplane, your competitors are to your left, your right and immediately behind you, reading whatever you have in front of you. If that is your laptop, displaying presentations or documents relative to your business, you can be sure they are taking notes and the information is going to be used to your company's detriment.

The cost to the Company for data disclosed through unauthorized access is the value of current and potential business lost as a result. While difficult to objectively quantify, the loss can be considerable, especially if the instance of the loss becomes public knowledge. If a back door application provided the means of unauthorized access, the costs include

- Cost of disinfecting (if possible) the system or
- Cost of re-imaging the system with the standard image and work products; and
- Downtime incurred by the consultant while the system is cleansed of the worm, virus or trojan, or a replacement system is configured, imaged and shipped out.

The CSI/FBI Survey lists the annualized loss through theft of proprietary information as reported by 41 of their respondents.

#### **1.4.5 Loss through propagation of problems to other systems**

While the Company has tools on its internal networks to prevent the spread of viral infections and worms, and regularly updates its tools to maintain currency, practice in the field cannot be controlled centrally. The Company uses Lotus Notes as a secure email system for all Company business and the Company actively scans all incoming and outgoing email for viruses. The Company has licensed a commercial anti-virus scanner that is installed and initially configured in the standard image placed on each laptop and the Company regularly scans its internal servers for malware. Access to the Company's

internal network is provided through controlled VPN access via a public ISP and all traffic over the VPN is scanned before it hits the Company net.

However, since the policy specifically restricts the use of the Company's email system and the Company provided ISP account to "official use only" by requiring the user to identify his/herself as an employee of the Company in the email, the consultant in the field must rely on other mechanisms for personal email. It is reasonable to assume every consultant has at least one personal email account not subject to the controls enforced by Notes, and it is likely that consultants might be web surfing on their own time in the evenings, using their personal ISP accounts. Both of these practices are ripe vectors for infection. Unlike scanned Company provided communication channels, these channels may permit exporting infection to others, including business partners and clients. This could also include malware exported by the laptop to client networks to which the consultant is connected while on assignment.

The cost to the company for problems propagated to other systems is difficult to measure directly, but the impact on the company's image can be very great. The direct costs to the company would include:

- Cost of disinfecting (if possible) the system or
- Cost of re-imaging the system with the standard image and work products; and
- Downtime incurred by the consultant while the system is cleansed of the worm, virus or trojan, or a replacement system is configured, imaged and shipped out.

#### **1.4.6 Loss through financial liability accrued by consultant**

Although the company imaged the system with a wealth of useful software and believes the software on the system is sufficient for almost any assignment, the individual consultant may disagree and download or install additional software onto the laptop. Section 7.4 of the company policy permits this, providing such software is properly licensed, used in accordance with the license and the downloading/installation thereof does not introduce malware into the machine or the company's networks.

Violating these limitations raises the potential for loss in two distinct ways. The first is the introduction of malware, the risks of which are discussed above in Sections 1.4.3 through 1.4.5. The second means is potentially much more damaging and that is the use of unlicensed software or software that is used outside the scope of its license. The risk here invites a Software Publishers Association audit of the company's licensing policy and the use of software on all machines within the company. Unlawful use of licensed software can result in the company

- Covering the cost of a company-wide audit of software usage;
- Buying legal copies of all such software used for all users within the company who would be performing the same function as the consultant, at full MSRP; and
- Paying a considerable fine and, if incurred, court costs.

### **1.4.7 Loss through degradation of consultant/company image**

Consultants are often expected to perform online research at client sites and occasionally deliver presentations to clients and management in which there is an Internet component. As most surfers of the Internet are aware, many sites do not manage advertising that appears on the site as rigorously as they should and advertisements and page referrals to sites are incompatible with Section 4.3 of the policy. While this can be explained, having an X-rated picture suddenly flash up while doing research in a client's office is embarrassing and adversely affects both the consultant's and the company's image. At certain clients, blocking software might trap the page referrals resulting in a formal warning to the offender and/or client contact. The cost of this loss is to credibility and reputation.

## **1.5 Mitigation of Above Risks**

The basis of the audit is to determine whether mitigation sufficient to offset a risk is in place and, equally important, whether a process is in place to maintain that sufficiency over time.

### **1.5.1 Outright loss of laptop**

Vigilance is the primary form of mitigation to offset this risk. Additional steps that can be taken to reduce the likelihood of theft and reduce the likelihood of the thief being able to access the data on the system if taken include:

- Availability and proper use of lockdown cable
- Disabling floppy and CD boot access
- Strong boot and system login password
- "Secure" file system
- Labeling of equipment
- Adequate recent backup

### **1.5.2 Loss of data through disk/system failure or deletion**

While the eventual failure of the system is inevitable, steps can be taken to mitigate both the loss and the inconvenience attendant to a system failure:

- Disk failure warning diagnostic tools
- Adequate recent backup

### **1.5.3 Loss of system integrity through infection by viruses**

With apparently no end in sight to the stream of ever-enhanced viruses, worms and trojans targeting both published and unpublished vulnerabilities in operating systems and applications, the best defense is protection in depth. The set of defenses employed in the system to mitigate this risk must include:

- System and applications updated to most recently approved patch level

- Antivirus software and virus tables updated to most recently approved level, configured properly and running
- Updated software firewall in place, configured properly and operating
- Demonstrable process in place to ensure timely application of updates to system, applications, antivirus software and firewall
- Adequate recent backup

#### **1.5.4 Loss of security of data through unauthorized access**

There are at least two ways to access the system, through the keyboard or some form of interconnect, both modes must be guarded as follows:

- Strong boot and login passwords
- Mandatory lock of system after inactivity
- System and applications updated to most recently approved patch level
- Antivirus software and virus tables updated to most recently approved level, configured properly and running
- Updated software firewall in place, configured properly and operating
- Demonstrable process in place to ensure timely application of updates to system, applications, antivirus software and firewall
- Adequate recent backup

#### **1.5.5 Loss through propagation of problems to other systems**

Propagation usually occurs because the consultant's laptop was infected by malware through one of several vectors. Restricting email from hosts other than the company's Lotus Notes email system to be text only and the rigorous scanning of all software before it is installed and all inbound email will reduce the likelihood of infection that will result in propagation.

- System and applications updated to most recently approved patch level
- Antivirus software and virus tables updated to most recently approved level, configured properly and running
- Updated software firewall in place, configured properly and operating
- Demonstrable process in place to ensure timely application of updates to system, applications, antivirus software and firewall
- Configuring an additional email client, if installed, to accept and generate only text email, or installing a filtering proxy to eliminate non-text email
- Configuring the browser(s) to automatically scan all downloads for viruses

#### **1.5.6 Loss through financial liability accrued by consultant**

The liability here is incurred through the installation of unlicensed software and the most direct form of mitigation is to require the consultant to provide evidence of legal license for each piece of software on the Desktop or in the Start menu that is not included in the company's standard image. Were the laptop connected to the company's network, it

would be possible to automatically scan the machine for software not appearing on either the Desktop or the Start menu, producing a list of software to check for license.

### 1.5.7 Loss through degradation of consultant/company image

Loss of image in this instance can best be mitigated by the installation and timely updates of an advertisement and popup blocker.

## 1.6 Mapping of Mitigations to Company Policy

Reviewing the company policy on communications systems and media to identify the relevant sections and map the intent of those sections into a set of requirements applying to computing equipment in general is difficult. Generalizing those requirements to laptops, devices that are completely outside the company's protective firewall and thus subject to more direct attack, is a stretch. Nonetheless, the following table is my attempt at mapping the various mitigations identified in section 1.4 above to specific policy sections.

**Table 1 – Risk/Mitigation identified in Company Policy**

	Policy Sections													
Mitigation	4.3	4.5	4.7	6.1	6.3	6.4	7.1	7.2	7.3	7.4	7.6	7.7	7.9	7.10
Physical					X	X						X		
Passwords					X	X		X			X	X		X
Boot sequence					X	X						X		
Antivirus					X	X	X		X	X		X		
Firewall		X			X	X	X		X			X		
Ad filter	X													
Backup				X	X							X		
Disk health status												X		
Email clients		X	X		X	X	X	X	X		X	X		
User software									X	X			X	
Operating system					X	X			X			X		X
Applications					X	X			X			X		
File system					X	X			X		X	X		
Browser	X								X	X		X		
VPN / Dial Access					X	X		X	X					

## 1.7 Base System Configuration

The laptop of choice for the Consulting Group at this time is the IBM 600X Laptop running Windows 2000/SP2/SR1 on the NTFS file system. Included with the system is a 10/100 Ethernet card and external floppy drive. The system has an internal modem and CD-ROM drive. A user account with administrator privileges and a system administrator



account are installed. The rationale for providing the user with administrator privileges is that many software packages cannot be installed, nor can hot-fixes or service packs applied without administrator privilege, a serious shortcoming in the industry.

The software suite pre-installed on the system includes

- Microsoft Office 2000 Professional/SR-1
- Visio 2000/SR-1
- Lotus Notes v5.09a
- Netscape v4.78 with AIM
- AT&T Global Dialer
- Cisco VPN client
- Adobe Acrobat Reader
- Internet Explorer 5.5
- Lotus Notes 5.04a
- NetMeeting 3.01
- NetSwitcher II
- Norton Antivirus 7.5
- WinZip 8.1
- Methodology toolset of templates

To this, the consultant may add applications necessary for specific engagements or those personal applications for which s/he can show evidence of valid license.

## 1.8 Assessment Tools

To perform the self-assessment, in addition to the applications themselves, several Microsoft tools will be used. These include:

- Microsoft Windows Update <<http://windowsupdate.microsoft.com/>>
- Microsoft Office Update <<http://office.microsoft.com/productupdates>>
- Microsoft Baseline Security Analyzer  
<[http://www.microsoft.com /security/tools/Tools/MBSAWP.asp](http://www.microsoft.com/security/tools/Tools/MBSAWP.asp)>

## 2 Assessment/Audit Process

This section presents the step-by-step process for the self-assessment, identifying the characteristics to look for, giving examples where appropriate and providing some context in which the step makes sense.

We'll start the checklist from the outside of the laptop and work our way further into the laptop as we go along. Once the machine is up and running, you will need to connect to the Internet to check for specific updates.

### 2.1 Physical Security

Reference	“Locking Down the Laptop,” Paul Korzeniowski, <b>Information Security</b> , February 2001, <a href="http://www.infosecuritymag.com/articles/february01/features_laptop_security.shtml">http://www.infosecuritymag.com/articles/february01/features_laptop_security.shtml</a> ; Company Policy Section 7.7, Appendix A
Objective	Identify precautions taken to prevent loss
Risk	Moderate
Compliance	Yes to 2.1.1a, 2.1.2b, 2.1.3a-c and an Asset Code number for 2.1.2a
Testing	See description and questions below
Mode	Objective: 2.1.1a, 2.1.2a-b, 2.1.3a-b Subjective: 2.1.3c

#### 2.1.1 Laptop Bag Identification

The airlines' admonition “Bags look alike” is doubly true with regard to laptop cases and the little business card tags do little to provide clear differentiation from a distance of this clear target of theft. To reduce the possibility of theft while in transit, the consultant is instructed to write his/her name in bold gold or silver block letters at least 2” high, clearly readable from 10’ on the outside of the bag. Paint pens are available in the office or from most stationers. Laptops shall not be checked as luggage.

a. Is the laptop bag labeled with your name in print sufficiently large that it can read from at least 10’ away?	
--	--

#### 2.1.2 Asset Identification

Each laptop is identified with a company bar-coded asset tag. In the event the consultant may undertake overseas assignments, the laptop will also have affixed to its bottom an International Warranty sticker bearing the name of the company and the laptop's serial number. If you require an International Warranty, call the IBM Help Line for the form.

a. What is the number on the bar-coded asset tag?	
---	--

b. If you can anticipate going abroad, does your laptop have an IBM International Warranty Registration sticker on the bottom?	
--	--

### 2.1.3 Physical Lockdown

To prevent the loss of the laptop while it is exposed, the consultant is provided with a cable lock suitable for attaching the laptop to a desk or other non-portable object

a. Do you have a lockable cable for attaching your laptop to a relatively non-portable object?	
b. Demonstrate that you know how to attach the cable to your laptop.	
c. Do you, as a matter of practice, lock your laptop down whenever it may be unattended?	

## 2.2 Boot Process

Reference	Laptop Security Guidelines, LabMice.Net, <a href="http://www.labmice.net/articles/laptopsecurity.htm">http://www.labmice.net/articles/laptopsecurity.htm</a> ; Company Policy Section 7.2, Appendix A
Objective	Prevent unauthorized personnel from accessing data on laptop
Risk	Moderate
Compliance	Yes to 2.2.1a-b and 2.2.2a
Testing	See description and questions below
Mode	Objective: 2.2.1a-b, 2.2.2a Subjective: None

### 2.2.1 Boot Password

Plug in and turn on the laptop. **Press** the **F1** key down as it is displaying the RAM counter.

a. Does the laptop ask you for a boot password?	
b. Does the password conform to the guidelines in Section 7.2 of the Policy?	

If not, **Click** on the **Password** box and then **click** on the **Power On** button, following the prompts to set a password. **Exit** back to the main boot menu screen.

IBM's ThinkPad Support Site cautions: "Do not forget your Power On Password! If you forget your power-on password, you cannot reset it. You have to take the computer to an IBM authorized reseller or IBM marketing representative to have the password cancelled.

Proof of purchase is required, and an additional charge might be required for the service.”<sup>5</sup>

## 2.2.2 Boot Devices

After **Exiting** back to the **main boot menu** screen, **click** on the **Power On** box and check which devices are “numbered” in the order they will be checked.

a. Does the laptop permit booting only from the internal disk, i.e., are floppy and CD devices unchecked?	
---	--

**Exit** and **restart** the laptop.

## 2.3 System Password

Reference	“Accounts with No Passwords or Weak Passwords,” <b>The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts’ Consensus</b> , Version 2.503 April 8, 2002, SANS Institute. “Checklist: Create Strong Passwords,” <b>7 Steps to Personal Computing Security</b> , Microsoft Corporation, <a href="http://www.microsoft.com/security/articles/password.asp">http://www.microsoft.com/security/articles/password.asp</a> ; Section 7.2 of Company Policy, Appendix A.
Objective	Ensure compliance with specific Company policy
Risk	Moderate
Compliance	Yes to 2.3a; less than 6 months for 2.3b; >4 for 2.3c
Testing	See description and questions below
Mode	Objective: 2.3a-c Subjective: None

As a minimum, there are four passwords to be configured on the laptop, each is to conform with Section 7.2 of the policy. This is the second:

a. Does your Windows 2000 login password conform to the guidelines listed in Section 7.2 of the Company Policy?	
b. How long ago was this password changed?	

On the tools CD is a zip file named Password.zip. Unzip this file to a temporary directory and open a DOS window, changing to the directory into which you unzipped the file. Run the application by typing “password” – the application will ask you to provide a password and you should supply one of the four passwords (boot, system login, Lotus Notes and the AT&T Dialer). You will run the program several times, once for

<sup>5</sup> “TP General - How to remove/add/change a power on password,” IBM ThinkPad Support Site, IBM Corp., <http://www.pc.ibm.com/qtechinfo/YAST-3JZNDP.html>

each password. Password.exe will test the supplied password using conventional password cracking technology and rate the relative “strength” of the supplied password.

c. What is the relative strength of the system login password?	
--	--

## 2.4 Antivirus Protection Status

Reference	“Checklist: Use Anti-Virus Software,” <b>7 Steps to Personal Computing Security</b> , Microsoft Corporation, <a href="http://www.microsoft.com/security/articles/antivirus.asp">http://www.microsoft.com/security/articles/antivirus.asp</a> ; “Anti-virus Test Files,” eicar Online, <a href="http://www.eicar.org/anti_virus_test_file.htm">http://www.eicar.org/anti_virus_test_file.htm</a> ; Company Policy Section 7.3, Appendix A
Objective	Ensure that the Company installed anti-virus software is up-to-date and properly configured
Risk	High
Compliance	Yes to 2.4a-s and 2.4v; No to 2.4t or an adequate explanation in 2.4u
Testing	See description and questions below
Mode	Objective: 2.4a-t, 2.4v Subjective: 2.4u

Out-of-date virus identification tables offer protection only against older viruses, while a misconfigured antivirus application may be providing no protection when you need it. **Open** Norton Antivirus and review the System Scanning Features.

a. Is “Auto-Protect” set to On?	
b. Is “Email scanning” set to On?	
c. Is “Script Blocking” set to On?	
d. Was the last “Full System Scan” conducted within the past week?	

In the “Virus Definitions Service” in the bottom half of the screen,

e. Is the date of the date of the “Virus Definitions” within the past two weeks and equal to or earlier than the date of the last “Full System Scan” above?	
f. Is “Automatic Update” set to On?	

**Select** Options/Norton Antivirus and examine the Auto-Protect screen.

g. Are the three boxes under “How to stay protected” all checked?	
h. Under “How to respond...” is the “Try to repair...” entry	

selected?	
i. Under "Which file types to scan..." is "Comprehensive..." selected?	

Select the Manual Scan screen

j. Are both boxes under "What items to scan..." checked?	
k. Under "How to respond..." is "Try to repair..." selected?	
l. Under "Which file types..." is "Comprehensive..." selected?	
m. Is "Scan within compressed files" checked?	

Select the Bloodhound screen directly under Manual Scan and

n. Is the "Enable Bloodhound" box checked?	
o. Is "Highest level of protection" selected?	

Select the Email Scanning screen and

p. Are both of the boxes under "What to scan" checked?	
--	--

Select the Activity Log and

q. Are all four boxes under "Which events to log" checked?	
--	--

Select the Miscellaneous screen and

r. Is the "Enable Office Plug-in" box checked?	
s. Is the "Alert me on start-up..." box checked?	

Close the **Option box** and select the **Reports entry** under Norton Anti-virus on the left. Click on the "**View Report**" button for the Activity Log. Click on the "**Filter**" button and, with only the "Virus Detections," "Access denied errors" and "Quarantine activities" checked, click on **OK**.

t. Does the Activity Log list any suspicious activity, e.g., viruses?	
u. If activity was listed, what is listed as the disposition?	

Open your browser and surf to the eicar online Anti-virus Test File webpage at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Attempt to download each of the four files at the bottom of the page.

v. Did the Anti-Virus program block the downloads and	
---	--

quarantine the files?	
-----------------------	--

## 2.5 Firewall Status

Reference	“Checklist: Install a Firewall,” <b>7 Steps to Personal Computing Security</b> , Microsoft Corporation, <a href="http://www.microsoft.com/security/articles/firewall.asp">http://www.microsoft.com/security/articles/firewall.asp</a> ; “Laptop Security Guidelines,” LabMice.Net, <a href="http://www.labmice.net/articles/laptopsecurity.htm">http://www.labmice.net/articles/laptopsecurity.htm</a> ; ShieldsUP!, Gibson Research Corporation, <a href="http://grc.com/default.htm">http://grc.com/default.htm</a> ; Company Policy Section 7.5, Appendix A
Objective	Ensure that software firewall is installed and correctly configured
Risk	High
Compliance	Yes to 2.5a-e
Testing	See description and questions below
Mode	Objective: 2.5a-e Subjective: None

In the above reference, Microsoft states, “Good fences make good neighbors. You can add an important layer of protection between your computer and the Internet by using a firewall system. Potential intruders scan computers on the Internet probing for a “port” where they can break and enter. A firewall can block unauthorized entry into your computer, as well as restrict outbound traffic.”

Included on the CD is an installable version of ZoneAlarm Pro, the firewall component of the new system image. In the event your system does not have this application already installed, do so now. Once it is installed, bring up the application. Like many applications, you will probably have to reboot to complete the installation.

a. In the box on the right side of the Overview/Status screen, does the app state that it is “up to date” or not?	
b. On the Firewall/Main screen, is the Internet Zone setting at High and the Trusted Zone setting at Medium?	
c. On the Alerts & Logs/Main screen, is Event Logging enabled and Program Logging set to High?	
d. On the Email Protection screen, is Mail Safe enabled?	

Start up your browser and go to the GRC site, <http://grc.com/default.htm>, selecting the ShieldsUP! link. Download the IP agent and run it to confirm your IP address. Click on the Test My Shields button and wait until the test is complete. After running the Test My Shields test, run the Probe My Ports test.

e. Were all of the ports listed as either Stealth! or Closed?	
---	--

## 2.6 Lotus Notes Protection

Reference	“Lotus Notes Frequently Asked Questions,” Division of Information Technology, Stony Brook University, <a href="http://clientsupport.stonybrook.edu/notes.shtml">http://clientsupport.stonybrook.edu/notes.shtml</a> ; “ID and Password Recovery,” <b>Notes Net</b> , <a href="http://www.notes.net/today.nsf/f01245ebfc115aaf8525661a006b86b9/2bc078be1aa6095285256af70059dd3a?OpenDocument">http://www.notes.net/today.nsf/f01245ebfc115aaf8525661a006b86b9/2bc078be1aa6095285256af70059dd3a?OpenDocument</a> ; Company Policy Section 7.1, 7.2 and 7.6, Appendix A
Objective	Ensure security of Company-wide email system
Risk	Low
Compliance	Yes to 2.6.1a and 2.6.2a; Acceptable to 2.6.1b
Testing	See description and questions below
Mode	Objective: 2.6.1a and 2.6.2a Subjective: 2.6.1b

### 2.6.1 Notes Passwords

Since your Lotus Notes ID file contains the encryption key for all of your email and losing your Notes ID file means that you will lose access to all stored email, you are encouraged to copy your Notes ID file, identified as “name.ID” where the name is your defined 8-character company shortname.

a. Have you created at least one floppy diskette or CD, stored safely at home, containing your Notes ID file?	
b. Does your Lotus Notes password conform to the guidelines listed in Section 7.2 of the Company Policy?	
c. Have you changed your Notes password since the last time you created a backup copy of your Notes ID file? (If not, create a new copy now)	

### 2.6.2 Notes Email Database Encryption

To prevent someone from opening your local replica of your Notes mailbox, it should be encrypted using at least medium level encryption. **Open Lotus Notes** and **right-click** on the **local copy** of your mailbox. **Select Database/Properties/Encryption Settings.**

a. Is the “Locally encrypt this database” button selected with Medium encryption?	
---	--

You may want to save your Lotus Notes desktop definition, desktop.nsf, and any local archives independent of your normal backup as you might wish to copy these files to a backup installation of Notes.



## 2.7 Operating System & MS-Office Status

Reference	Best Practices for Applying Service Packs, Hotfixes and Security Patches, Microsoft Corporation, <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secure.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secure.asp</a> ; “Checklist: Keep Software Up-To-Date,” <b>7 Steps to Personal Computing Security</b> , Microsoft Corporation, <a href="http://www.microsoft.com/security/articles/update.asp">http://www.microsoft.com/security/articles/update.asp</a> ; Company Policy Section 7.3 and 7.4, Appendix A
Objective	Ensure that security patches for recently discovered exploits are in place
Risk	High
Compliance	No to 2.7.1a-b, 2.7.2a
Testing	See description and questions below
Mode	Objective: 2.7.1a-b, 2.7.2a Subjective: None

### 2.7.1 Windows 2000 Update

From the Start menu, select **Windows Update** and, once the page has come up, **double click** on **Product Updates**.

a. Are any “Critical Updates and Service Packs” listed?	
b. Are any “Advanced Security Updates” listed?	

If there are any of the above, check the entries, download and install them. Because of the manner in which Microsoft handles updates, this may take several tries with reboots in between to get them all downloaded and installed.

### 2.7.2 Office 2000 Update

From the Windows Update page, **double-click** on the **Microsoft Office Product Updates** button on the left. It will perform a check of your machine against its database.

a. Are any “Security” or “Vulnerability” updates listed?	
--	--

Download and apply any of the above updates you find listed. No doubt you will have to reboot your system again.

## 2.8 Microsoft Baseline Security Scan

Reference	Company Policy Section 7.2, 7.3 and 7.4, Appendix A
-----------	---

Objective	Ensure that risks identified by Microsoft both in and in the use of their software are addressed
Risk	High
Compliance	None for 2.8b or satisfactory resolution provided in 2.8c
Testing	See description and questions below
Mode	Objective: 2.8a,b,d Subjective: 2.8c,e

From the MS\_BSA directory on supplied CD, install the Microsoft Baseline Security Analyzer. **Start** the application and **click** on “**Scan a computer**” from the Welcome screen. From the “Pick a computer to scan” screen, **highlight** your computer from the “Computer Name” scroll box. Make sure the “Check Windows Vulnerabilities”, “Check Weak Passwords” and “Check Hotfixes” boxes are checked. **Click** on “**Start scan**” at the bottom.

a. What was listed as the overall Security Assessment?	
b. What items were listed as “Red” vulnerabilities?	
c. What steps were taken to correct the Red vulnerabilities?	
d. What items were listed as “Yellow” vulnerabilities?	
e. What steps were taken to correct the Yellow vulnerabilities?	

## 2.9 Additional Email Client

Reference	“A quick guide to email security,” Paul Slavic, <a href="http://www.zzee.com/email_security">http://www.zzee.com/email_security</a> ; “Virus Check.” Zimbabwe OnLine Services, <a href="http://www.virustest.co.zw/">http://www.virustest.co.zw/</a> ; Company Policy Section 7.1, 7.9, Appendix A
Objective	Ensure that an alternate email client does not decrease the level of security provided for the applications and data on the laptop
Risk	High
Compliance	Yes to 2.9c, 2.9d
Testing	See description and questions below
Mode	Objective: 2.9c-d Subjective: 2.9a-b

If you are using an additional email client you should set it to not accept or display HTML-formatted messages or messages sent in Rich Text format. Both of these formats are capable of hiding malware (viruses and such) or invisible links to malware.

If your alternate email client is Outlook or another email client that defaults to enhanced message formatting, you should give serious thought to downloading and registering

ZZEE's **Email Not HTML** proxy at <http://www.zzee.com>. To quote from their description,

Email worms, viruses, trojans, web bugs? They can come to you right with HTML-based emails. Protect from these threats while keeping the message readability and without information loss. The program replaces HTML by clear text and moves HTML to attachments. It also zips all suspicious attachments, so executable files can't be launched automatically. It works with any POP3 email software. This program is the first in the world in its class!<sup>6</sup>

a. Are you using an email client in addition to Lotus Notes, e.g. Outlook or Eudora?	
b. What client is it, name and version?	
c. Have you disabled the client's acceptance of HTML-formatted and Rich Text messages?	

Start up your default browser and surf to <http://www.virustest.co.zw/><sup>7</sup>. This site provides an automated email check of your antivirus protection. Enter your personal email address at the bottom of the page and press enter. Several minutes later, several messages will be sent to your email address containing the eicar test files<sup>8</sup>. Assuming your email program and the antivirus utility is configured correctly, these messages should be intercepted by the antivirus program.

d. Are your email client and the supplied antivirus utility correctly configured to intercept a messages sent from ZOL containing the eicar virus test string?	
--	--

## 2.10 System/File Backup

Reference	"G3 - Non-existent or Incomplete Backups," <b>The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts' Consensus</b> , Version 2.503 April 8, 2002, SANS Institute; "Laptop Security Guidelines," LabMice.Net, <a href="http://www.labmice.net/articles/laptopsecurity.htm">http://www.labmice.net/articles/laptopsecurity.htm</a> ; Company Policy Section 7.7, Appendix A
Objective	Ensure that data and applications are not lost
Risk	Low (but consequences of risk are very high)
Compliance	Descriptions indicate likelihood of recovering data
Testing	Provide description of practice/usage

<sup>6</sup> "ZZEE Email Not HTML: gracefully handles HTML based email,"  
[http://www.zzee.com/enh/#zzee\\_link\\_3\\_1014864770](http://www.zzee.com/enh/#zzee_link_3_1014864770)

<sup>7</sup> "ZOL Anti-Virus Test," Zimbabwe OnLine Services, <http://www.virustest.co.zw/>

<sup>8</sup> "Anti-Virus test file," eicar online, [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

Mode	Objective: None Subjective: 2.10a-e
------	--

Recognizing that in the event of a failure of your system, e.g., hard disk crash, corrupted or virus infected disk or theft of laptop, your office can only provide you with a newly imaged system containing none of the work products or personal files you currently have on your system, consider the consequences such failure. Remember, the company holds you personally responsible for the backup and protection of work products existing solely on your system. Consider how long your system will be inaccessible while it is being re-imaged.

a. Describe the process you use to backup work-related data and application files?	
b. What program/package/utility, including version number, do you use for the process?	
c. What is the scope of the backup, i.e., work data files only, data and apps, or complete system backup?	
d. How often or according to what schedule do you exercise this process?	
e. Have you exercised the recovery/restore feature of your backup, both partial and the full scope?	
f. What was the result of the above recovery/restore?	

## 2.11 ISP Dialer

Reference	Company Policy Section 7.2, Appendix A
Objective	Ensure security of Company-provided ISP account
Risk	Low
Compliance	Yes to 2.11a-b
Testing	See description and questions below
Mode	Objective: 2.11a-b Subjective: None

**Startup** the AT&T dialer and when the initial screen comes up

a. Does your AT&T Global dial-in password conform to the requirements stated in Section 7.2 of the Company Policy?	
b. Is the "Save Password" box unchecked?	

## 2.12 User Installed Applications

Reference	"Anti-Piracy FAQ," Software & Information Industry Association,
-----------	---

	<a href="http://www.spa.org/piracy/faq/default.asp">http://www.spa.org/piracy/faq/default.asp</a> ; Company Policy Section 7.4 and 7.9, Appendix A
Objective	Ensure that adequate license exists for all applications on Consultant's laptop
Risk	High
Compliance	Yes to 2.12a
Testing	Provide examples of registration screens as directed
Mode	Objective: 2.12a Subjective: None

For each and every application, program, system, data set or file you have installed on your laptop that appears either on the Desktop or in the Start Menu, beyond what was contained in the image provided originally with the machine, answer the following question:

a. Can you provide either a paper license or a screen capture of a registration screen that indicates the program is licensed to you?	
---	--

In the event the answer is "No" for any application, program, system data set or file, you are required to remove it from your company provided laptop. You should consider collecting these together in case your machine ever comes into the office to be refreshed.

© SANS Institute 2000 - 2002

### 3 An Application of the Assessment Process

The following is the documented results of an assessment on my laptop using the process described in Section 2 above. Among the items below are 10 that represent the most significant security concerns, in my opinion, with evidence to demonstrate the state in which the assessment items were found. These 10 items are identified in red. Four items were identified later as “stimulus/response” items, requiring evidence of test completion, and these are highlighted in yellow.

#### 3.1 Physical Security

##### 3.1.1 Laptop Bag Identification

a. Is the laptop bag labeled with your name in print sufficiently large that it can read from at least 10' away? (Item #1)	Yes, see Picture
--	------------------



Evidence 1 - Laptop Case Identification

##### 3.1.2 Asset Identification

a. What is the number on the bar-coded asset tag?	0027009
b. If you can anticipate going abroad, does your laptop have an IBM International Warranty Registration sticker on the bottom?	Yes

##### 3.1.3 Physical Lockdown

a. Do you have a lockable cable for attaching your laptop to a relatively non-portable object?	Yes
b. Demonstrate that you know how to attach the cable to your	See

laptop. (Item #2)	Picture
c. Do you, as a matter of practice, lock your laptop down whenever it may be unattended?	Yes



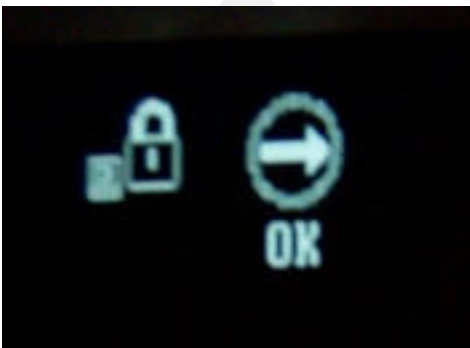
Evidence 2 - Laptop Lockdown Cable Use

## 3.2 Boot Process

### 3.2.1 Boot Password

a. Does the laptop ask you for a boot password? (Item #3)	Yes, see below
b. Does the password conform to the guidelines in Section 7.2 of the Policy?	Yes

Here is the OK after entering the boot password:



Evidence 3 - Successful Boot Password

### 3.2.2 Boot Devices

a. Does the laptop permit booting only from the internal disk, i.e., are floppy and CD devices unchecked?	Yes
---	-----

The machine is plugged into my SCSI tower and shows only physical disk drives as bootable; floppy and CD are not bootable:



Evidence 4 - Photograph of system manager screen

### 3.3 System Password

a. Does your Windows 2000 login password conform to the guidelines listed in Section 7.2 of the Company Policy?	Yes
b. How long ago was this password changed?	~6 months
c. What is the relative strength of the system login password?	5

Your rating was a 5 out of 10. Which is good however a very energetic hacker should be able to guess it.

Evidence 5 - Response from Password.exe

### 3.4 Antivirus Protection Status

a. Is "Auto-Protect" set to On? (Item #4)	Yes
b. Is "Email scanning" set to On? (Item #4)	Yes
c. Is "Script Blocking" set to On? (Item #4)	Yes
d. Was the last "Full System Scan" conducted within the past week? (Item #4)	Yes
e. Is the date of the date of the "Virus Definitions" within the past two weeks and equal to or earlier than the date of the last "Full System Scan" above? (Item #4)	Yes
f. Is "Automatic Update" set to On? (Evidence )	Yes





Evidence 6 - Antivirus Configuration

## Options/Norton Antivirus/Auto-Protect configuration

g. Are the three boxes under "How to stay protected" all checked?	Yes
h. Under "How to respond..." is the "Try to repair..." entry selected?	Yes
i. Under "Which file types to scan..." is "Comprehensive..." selected?	Yes

## Manual Scan configuration

j. Are both boxes under "What items to scan..." checked?	Yes
k. Under "How to respond..." is "Try to repair..." selected?	Yes
l. Under "Which file types..." is "Comprehensive..." selected?	Yes
m. Is "Scan within compressed files" checked?	Yes

## Manual Scan/Bloodhound configuration

n. Is the "Enable Bloodhound" box checked?	Yes
o. Is "Highest level of protection" selected?	Yes

## Email Scanning configuration

p. Are both of the boxes under "What to scan" checked?	Yes
--	-----

## Activity Log configuration

q. Are all four boxes under "Which events to log" checked?	Yes
--	-----

## Miscellaneous configuration

r. Is the "Enable Office Plug-in" box checked?	Yes
--	-----

s. Is the "Alert me on start-up..." box checked?	Yes
--	-----

## Activity Log Report

t. Does the Activity Log list any suspicious activity, e.g., viruses? (Item #5)	Yes, see below
u. If activity was listed, what is listed as the disposition? (Item #5)	Quarantine

As shown in the log below, Norton Antivirus reported four instances of the Klez virus in attachments to email. Curiously, the name of each of the attachments was different. Each of the emails was deleted from the email program.





Date: 4/21/2002, Time: 18:17:04, mhagerty on MHAGERTY  
The email attachment r172382[1].zlq is infected with the W32.Klez.gen@mm virus.  
The file was quarantined.

Date: 4/24/2002, Time: 8:08:24, mhagerty on MHAGERTY  
The email attachment only at.zl9 is infected with the W32.Klez.gen@mm virus.  
The file was quarantined.

Date: 4/24/2002, Time: 13:57:52, mhagerty on MHAGERTY  
The email attachment setup.zl9 is infected with the W32.Klez.gen@mm virus.  
The file was quarantined.

Date: 4/25/2002, Time: 18:36:58, mhagerty on MHAGERTY  
The email attachment bgcolor.zl9 is infected with the W32.Klez.gen@mm virus.  
The file was quarantined.

The attachments were moved to the quarantine folder as shown below:

File name ▲	Quarantined	Submitted	Status	Virus Name
 bgcolor.zl9	4/25/2002 6:36:26 PM	Not submitted	Quarantined	W32.Klez.gen@mm
 only at.zl9	4/24/2002 4:21:06 AM	Not submitted	Quarantined	W32.Klez.gen@mm
 r172382[1].zlq	4/21/2002 5:58:16 PM	Not submitted	Quarantined	W32.Klez.gen@mm
 setup.zl9	4/24/2002 1:57:31 PM	Not submitted	Quarantined	W32.Klez.gen@mm

## Evidence 7 - Quarantined Attachments

w. Did the Anti-Virus program block the downloads and quarantine the files?	Yes, see below
---	----------------



Evidence 8 - Indication of intercepted virus test file

### 3.5 Firewall Status

a. In the box on the right side of the Overview/Status screen, does the app state that it is “up to date” or not?	Yes
b. On the Firewall/Main screen, is the Internet Zone setting at High and the Trusted Zone setting at Medium?	Yes
c. On the Alerts & Logs/Main screen, is Event Logging enabled and Program Logging set to High?	Yes
d. On the Email Protection screen, is Mail Safe enabled?	Yes

ZoneAlarm Pro Log is attached as Appendix B.

f. Were all of the ports listed as either Stealth! or Closed?	Yes, see below
---	----------------

Port	Service	Status	4 Security Implications
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
22	SSH	Closed	
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Closed	Your computer has responded that this port exists but is

			currently closed to connections.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
135	RPC	Closed	Your computer has responded that this port exists but is currently closed to connections.
139	NetBIOS	Closed	Your computer has responded that this port exists but is currently closed to connections.
143	IMAP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
443	HTTPS	Closed	Your computer has responded that this port exists but is currently closed to connections.
445	MSFTDS	Closed	Your computer has responded that this port exists but is currently closed to connections.
5000	UPnP	Closed	Your computer has responded that this port exists but is currently closed to connections.

Evidence 9 - Port table from ShieldsUP! Probe My Ports

## 4.1 Lotus Notes Protection

### 4.1.1 Notes Passwords

d. Have you created at least one floppy diskette or CD, stored safely at home, containing your Notes ID file?	Yes
e. Does your Lotus Notes password conform to the guidelines listed in Section 7.2 of the Company Policy?	Yes
f. Have you changed your Notes password since the last time you created a backup copy of your Notes ID file? (If not, create a new copy now)	No (new diskette created within past 30 days)

### 4.1.2 Notes Email Database Encryption

a. Is the "Locally encrypt this database" button selected with Medium encryption?	Yes
---	-----

## 4.2 Operating System & MS-Office Status

### 4.2.1 Windows 2000 Update

a. Are any "Critical Updates and Service Packs" listed? (Item #6)	No
b. Are any "Advanced Security Updates" listed? (Item #6)	No

#### CRITICAL UPDATES AND SERVICE PACKS

No updates of this type are available at this time.

#### PICKS OF THE MONTH

No updates of this type are available at this time.

#### ADVANCED SECURITY UPDATES

No updates of this type are available at this time.

Evidence 10 - Windows Update Capture

### 4.2.2 Office 2000 Update

a. Are any "Security" or "Vulnerability" updates listed? (Item #7)	Yes
--	-----

These updates were listed. I have downloaded these four changes independently and attempted to apply them to my system, to which my system replies that these changes have already been made through the application of a larger update, yet Office 2000 Update continues to note them.

#### ■ Outlook 2000 SR-1: Extended E-mail Security Update (English version)

**You need the administrative version of this update due to previously applied administrative updates.**

This update is an extension of the original Outlook 2000 SR-1 Update: E-mail Security. If you installed this update before August 9, 2001, you should do so again in order to get the most recent security capabilities available. Last modified date: 9-August-2001.

[Detailed information about this update](#)

#### ■ Excel 2000 SR-1 Macro Modification Security Update – April 2002

**You need the administrative version of this update due to previously applied administrative updates.**

The Excel 2000 SR-1 Update: Macro Modification Security addresses a vulnerability that could allow malicious code to run in a Microsoft Excel file without warning.

Last updated: April-25-2002

[Detailed information about this update](#)

#### ■ Word 2000 Update: April 25 2002

**You need the administrative version of this update due to previously applied administrative updates.**

The Word 2000 Update: April 25 2002 offers you the highest levels of performance and security available for Microsoft Word. Last modified date: 25-Apr-2002.

[Detailed information about this update](#)

#### ■ PowerPoint 2000 SR-1 Macro Modification Security Update

**You need the administrative version of this update due to previously applied administrative updates.**

This update addresses a vulnerability that could allow malicious code to run in a PowerPoint file without warning. Last modified date: 3-Oct-2001.

[Detailed information about this update](#)

### Evidence 11 - Office 2000 Update Report

## 4.3 Microsoft Baseline Security Scan

From the MS\_BSA directory on supplied CD, install the Microsoft Baseline Security Analyzer. Start the application and click on “Scan a computer” from the Welcome screen. From the “Pick a computer to scan” screen, highlight your computer from the “Computer Name” scroll box and click on “Start scan” at the bottom.

e. What was listed as the overall Security Assessment? (Item #8)	Severe
f. What items were listed as “Red” vulnerabilities? (Item #8)	See below
g. What steps were taken to correct the Red vulnerabilities?	See below

(Item #8)		
h.	What items were listed as “Yellow” vulnerabilities?	See below
i.	What steps were taken to correct the Yellow vulnerabilities?	See below

✗	Windows Hotfixes	2 hotfixes are missing or could not be confirmed	What was scanned	Result Details	How to correct this
✗	File System	Not all hard drives are using the NTFS file system	What was scanned	Result Details	How to correct this
✕	Residual Anonymous	Computer is running with RestrictAnonymous = 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.	What was scanned		How to correct this
✕	Administrators	More than 2 Administrators were found on this computer	What was scanned	Result Details	How to correct this
✕	Password Expiration	All user accounts (2) have non-expiring passwords.	What was scanned	Result Details	How to correct this
<b>Score</b>	<b>Issue</b>	<b>Result</b>			
✕	Macro Security	4 Microsoft Office product(s) are installed. Some issues were found.	What was scanned	Result Details	How to correct this

#### Evidence 12 - MBSA Report

As shown above, there were two “Red” problems and four “Yellow” issues. Below is the description of the problems/issues with a discussion of the resolution. The last item above, the Macro Security fixes are discussed above in Section 3.7.2.

Score	Hotfix	Description
✗	<a href="#"><u>MS02-001</u></a>	Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data
✕	<a href="#"><u>MS01-022</u></a>	WebDAV Service Provider Can Allow Scripts to Levy Requests as User

The above two hotfixes were downloaded in response to the first Red item, the Hotfixes report. Both of the hotfixes were then applied, but the first hotfix was rejected with a note indicating it was included in the already applied Windows 2000 Security Roll-up Package 1. The second hotfix could not be successfully applied as the system had already been “stepped” beyond the fix.

## Not all hard drives are using the NTFS file system.

### Result Details

Score	Drive Letter	File System
✓	C:	NTFS
✓	D:	NTFS
✓	E:	NTFS
✓	F:	FAT
✓	N:	NTFS
✓	P:	NTFS
✓	R:	NTFS

Paragon's Drive Backup, the tool I use to perform the partition-by-partition backup, must be run from DOS in order to capture entire NTFS partitions without any locked files. I decided that running it from a 7M DOS partition on the hard disk was less of a risk than permitting a floppy boot as the Power On boot password was limiting access to the disk.

## More than 2 Administrators were found on this computer.

### Result Details

Score	User
✗	\S-1-5-21-1121284804-1306546573-1232828436-1766
✗	\S-1-5-21-2107716844-1550652909-134157935-12948
✗	Administrator
✗	mhagerty

As noted in the Policy, I am required to retain the Company Administrator account so that the laptop can be examined periodically.



## All user accounts (3) have non-expiring passwords.

### Result Details

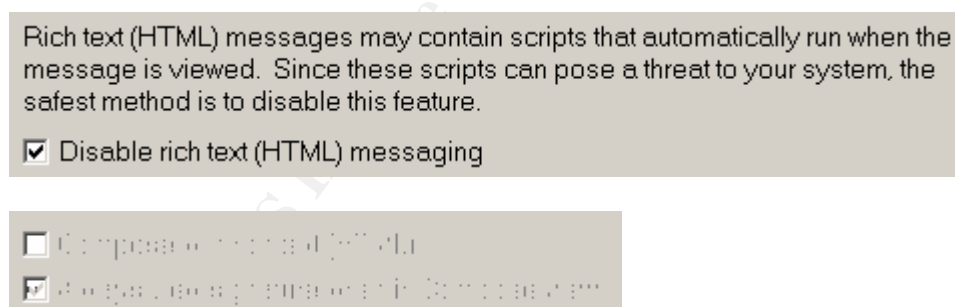
Score	User
X	Administrator
X	Guest
X	mhagerty

Windows 2000 has an issue with forcing password updates when the laptop is not connected to the Company LAN. As a consequence, the passwords are updated and synchronized when I bring the laptop to the office. The Guest account is disabled.

## 4.4 Additional Email Client

a. Are you using an email client in addition to Lotus Notes, e.g. Outlook or Eudora?	Yes
b. What client is it, name and version?	Calypso v3.30.00
c. Have you disabled the client's acceptance of HTML-formatted and Rich Text messages? (Item #9)	Yes

The following screen capture is from the configuration of Calypso:



**Evidence 13 - Disabled Rich Text (HTML) Messaging**

d. Are your email client and the supplied antivirus utility correctly configured to intercept a messages sent from ZOL containing the eicar virus test string?	Yes, see below
--	----------------

The following screen capture is from the Norton Anti-Virus popup on encountering the test message:



Evidence 14 - Intercepted virus

## 4.5 System/File Backup

a. Describe the process you use to backup work-related data and application files?	See below
--	-----------

I perform backup and full verify of the entire contents of the laptop to tape each week (Saturday night) with NovaBackup v6.60. The complete backup fits on one NS20 tape and the set of tapes is rotated so that four are used in succession for weekly backups with the fourth one rolled into a set of three monthly backups. I examine the error log the following morning.

```

Full Backup
1 1 ☒ ☐ 04/18/2002 23:18 91454 8,143.6M
Full Backup of 600E
1 1 ☒ ☐ 04/27/2002 21:50 99096 8,674.1M
  
```

I perform a differential backup and verify of changes since the last full backup each night to a portable SyJet drive with NovaDisk v6.60. I examine the error log the following morning.

Before making changes to the system, e.g., applying a Service Pack or installing a new application, I perform a copy of all partitions on the laptop to a personally owned spare disk drive using Paragon Drive Backup v5.0. This operation is performed once a week at a minimum.

The reason for using the Paragon utility to create a partition-by-partition backup rather than an "image" file backup is quite simple. If the primary disk fails for whatever reason, the backup disk drive can be substituted, the differential backup changes restored and the system is back up and running within an hour. Yes, it has happened, and securing a replacement disk drive from IBM took 48 hours. If I had required the system to be re-imaged, it would have required me to fly home afterwards to restore all of the data and additional applications from tape.

b. What program/package/utility, including version number, do	NovaStor/
---	-----------

you use for the process?	NovaDisk
c. What is the scope of the backup, i.e., work data files only, data and apps, or complete system backup?	See a.
d. How often or according to what schedule do you exercise this process?	See a.
e. Have you exercised the recovery/restore feature of your backup, both partial and the full scope?	Yes, both
f. What was the result of the above recovery/restore?	See below

When I began using NovaStor's product there were several problems that did not become apparent until the disk crashed. While all of the data files were recovered from the backup tape onto a new disk, the operating system itself appeared incomplete. I don't know of a better way to describe it as other than "incomplete" as it would crash without warning and there were "cosmetic" differences that led me to believe the entire registry was not being either backed up or restored correctly. I rebuilt the system following guidance from the office, configuring it according to their recommendations, and reinstalled all of the apps, restoring only the data files from tape.

I contacted NovaStor and worked closely with their Tech Support department for about two months. Using a spare drive borrowed from the office, I performed a full backup followed by a full restore of the contents of the tape to the spare drive each time I received an updated test version. Once the problems were worked through I returned the spare drive and continued the regular schedule listed for a. above.

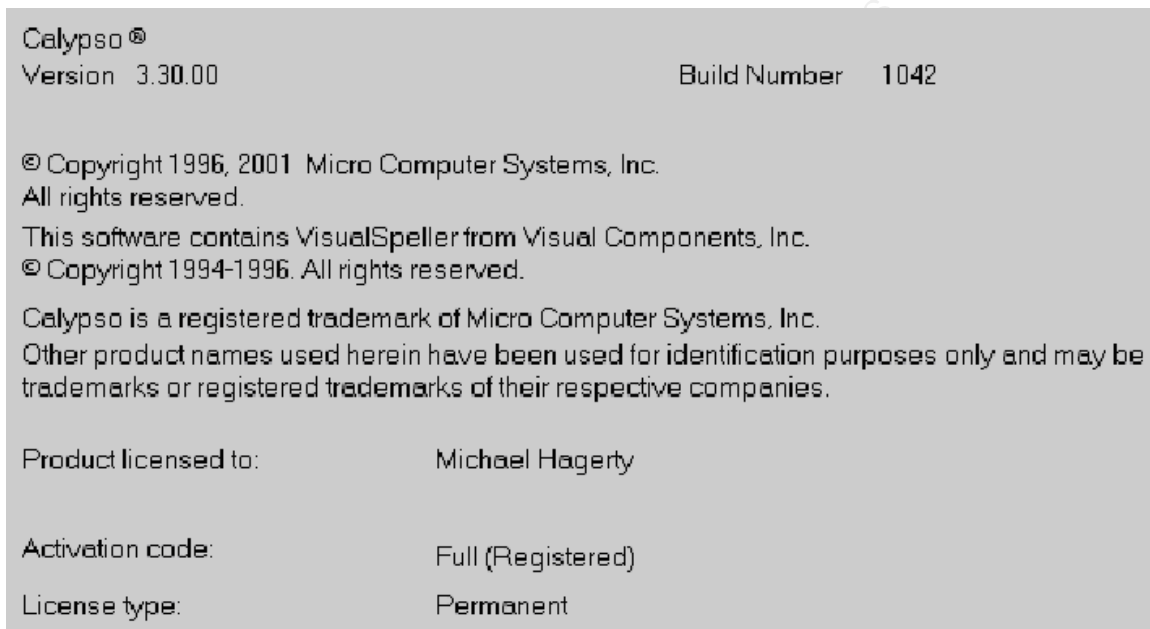
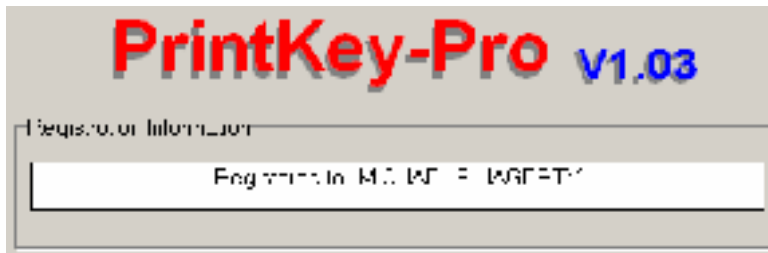
#### 4.6 ISP Dialer

c. Does your AT&T Global dial-in password conform to the requirements stated in Section 7.2 of the Company Policy?	Yes
d. Is the "Save Password" box unchecked?	Yes

#### 4.7 User Installed Applications

a. Can you provide either a paper license or a screen capture of a registration screen that indicates the program is licensed to you? (Item #10)	Yes
--	-----

## Evidence 15 - Example Registration Screens



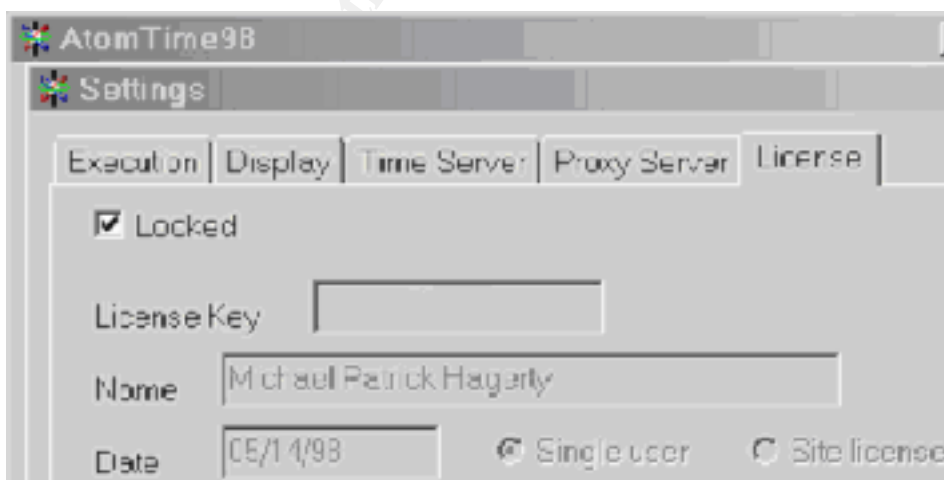
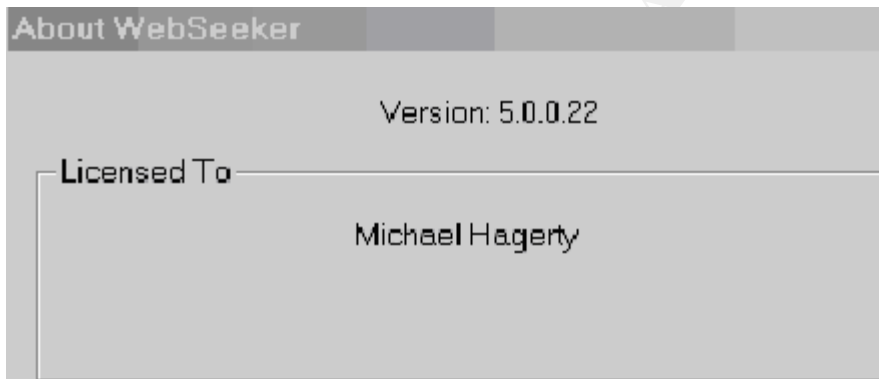
Registered to  
Michael Hagerty  
Single User License

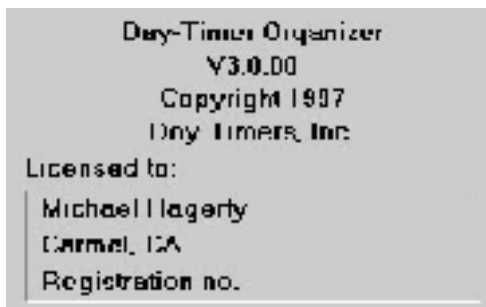


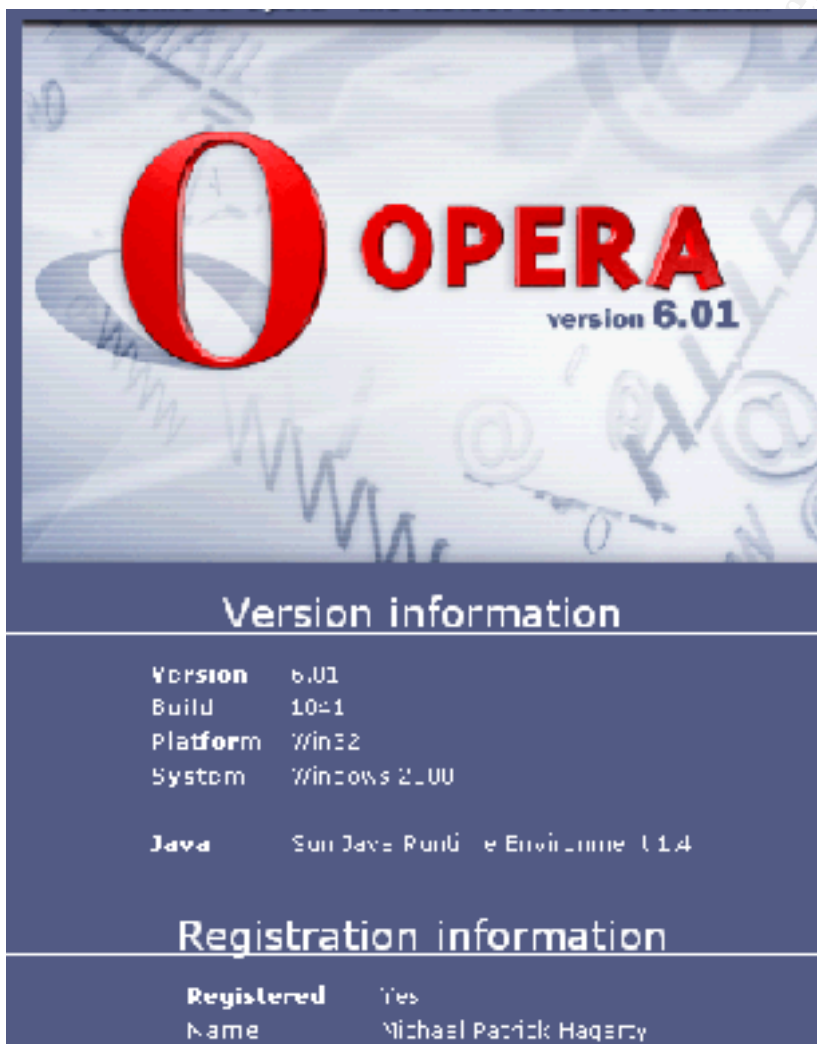
Licensed to: **Michael P. Hagerty**



# Adobe® Photoshop® Elements







## 4.8 Is the Laptop Securable?

Based on the above assessment, assuming that the base image was secure to begin with, the laptop is not appreciably less secure than it was first received. The assessment fulfilled the goal of providing a reasonable exercise for a consultant to perform in the field to determine whether he was acting with diligence toward maintaining security.

Is the assessment adequate for determining whether the consultant is behaving responsibly with regard to security? No. Nor is this simple assessment sufficient to determine whether changes to the underlying image need be made to improve the overall level of security. I have looked at the laptop configuration independently of the above assessment and note some areas in which certain issues have been sidestepped or ignored in the original image, e.g., LANMAN is supported despite the fact that this dramatically reduces password strength as the Company network supports Win9X systems.

Were the **control objectives** met through this process? I believe the answer is a qualified affirmative, if for no other reason than the assessment process will heighten the consultant's awareness of security and the need to protect the information contained on the laptop. A competent system administrator at a Company facility could do obviously much more, however the objective was to raise the bar up from no checking at all.

Could the system be made "secure" such that the risks, especially with regard to physical security could be eliminated? Sure, but to do so would deny the consultant a valuable resource and limit his/her effectiveness. Locking down the laptop and providing the consultant only a non-administrator account would discourage the consultant from finding ways in which innovative solutions could be deployed as well as make the system non-updatable in the field, due to Microsoft's insistence that all patches, hotfixes and service packs have to be applied from an administrator account.

The cost associated with the self-assessment is about two hours of the consultant's time, most likely during the evening and the cost of any additional security enhancing tools the Company would like to add to the image. Not an unreasonable tradeoff.

## 4.9 Is the System Auditable?

The self-assessment steps were clear, although screen shots of the various steps would help those who are more visual in identifying what they needed to do. Was the assessment sufficient to evaluate the security of the system? Given the constraints described above, yes; independent of the constraints, probably not. However, given the level of existing computer savvy and the likelihood that unskilled consultants would severely corrupt the system by making registry hacks, requiring the return of the laptop to the office (which this process is established to prevent), it is a reasonable tradeoff.



One of the major shortcomings of the self-assessment process is its reliance upon tools provided by Microsoft. Recent articles<sup>9</sup> indicate that the tools suffer from reporting both false positives and false negatives. The assessment conducted in this effort encountered six items that Microsoft indicated as needing updating, yet all of them had already been corrected through other patches. The above reference quotes the Microsoft Director of Security Assurance, “We need consistency and clarity across these tools.” Unfortunately, this is not yet true. However, given widely circulated pronouncements by Microsoft of their new security awareness, a set of reliable tools is potentially achievable and may, in the fullness of time, become widely available.

---

<sup>9</sup> “Security tool leaves holes,” **eWeek**, Volume 19, Number 16, April 22, 2002.

## 5 Follow Up to the Self-Assessment

### 5.1 Summary

I conducted an assessment of the Company-owned laptop provided to me as part of my consultant's toolkit using the self-assessment checklist listed in Section 2, with detailed results provided in Section 3. The assessment identified several areas in which the reporting tools erroneously indicated fixes were necessary despite their already having been applied. At least one instance of a serious problem was identified, i.e., a FAT formatted partition instead of the recommended NTFS format. The problem was created as an artifact of a complete backup solution. The benefit of an instantly recoverable backup appears to outweigh the risk of loss created by the problem. The system thus meets the criteria established for the assessment and appears to preserve a level of security comparable to the original image at the time it was created.

### 5.2 Identified Problems

Potential security problems were identified from three sources, Norton Antivirus, Microsoft Office 2000 Update and the Microsoft Baseline Security Analyzer (MBSA).

Norton Antivirus recorded four instances of the [W32.Klez.gen@mm](#) virus in attachments, all of which were correctly sent to the Quarantine folder. Microsoft Office 2000 Update and the MBSA, however, provided erroneous information, listing problems that either had already been corrected or suggested updates that could not be applied.

The MBSA correctly identified four potential security issues:

- RestrictAnonymous was not set to maximum
- A non-NTFS (i.e., FAT) partition was used
- More than 2 administrator accounts were present
- Three passwords were set to non-expire

In the first one, the RestrictAnonymous system variable was set to "1" rather than the recommended maximum setting of "2". To quote the MBSA Report, "This level prevents basic enumeration of user accounts, account policies, and system information." Details on the advantages and problems that may be encountered by setting RestrictAnonymous to the maximum level are explained by Microsoft in one of their "Q" papers, "How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261)."<sup>10</sup> I had previously done some experimentation with this setting, attempting to move it to the maximum, but encountered problems when attempting to browse to a

---

<sup>10</sup> "How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261)", Microsoft Product Support Services, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q246261>

client's network during an assignment. Therefore, the benefit of the middle level choice appears justified.

The second item, retaining an insecure FAT partition is more problematic. It is definitely possible to boot to DOS on this system, although the only utility that is provided on the FAT partition is the partition backup utility. The partition exists only to permit the making of a partition-by-partition backup. Almost all backup programs for Windows 2000 NTFS partitions which run under Windows 2000 suffer from the inability to capture an exact copy of the disk as Windows 2000 has numerous system files and logs open. The act of backing them up causes changes to the logs themselves. The utility chosen to provide this partition-by-partition backup runs on DOS and none of the files on the NTFS partitions are open. The fact that this was done to facilitate the complete restore of a previous backup within two hours in the field, negating the need to return the system to the office with the resulting non-billable downtime, seems reasonable.

The third and fourth potential security issues identified, having more than one administrator account on the laptop and having non-expiring passwords, are artifacts both of the Policy and of the only occasionally connected to the Company network nature of a laptop. The Policy requires a Company administrator account on the system, the Policy forbidding its removal. Microsoft requires that a user attempting to apply service packs, hotfixes and patches must be logged in as an administrator. To permit the application of these extremely valuable (and only too frequent) corrections to security holes in Windows 2000 and the MS Office 2000 products, the user in the field requires an administrator account. Synchronization problems have dictated the non-expiration of the passwords on these accounts.

### 5.3 Risk

While it is conceivable that an attack could be successfully mounted against the laptop, and there is ample evidence of such attempts shown in the ZoneAlarm log provided in Appendix B, the presence of an updated software firewall and updated antivirus software on top of a system patched to the vendor's current recommended level when connecting through a dial-up line appears to minimize the risk. While this system is in use at home, it is connected to the Internet via DSL through a 2wire firewall, thus providing an additional level of defense, i.e., defense in depth.

It is also possible to boot the system to the DOS partition and then load some errant application from an external floppy disk. To do so would require physical access to the laptop and the power on password. Given that the laptop is physically locked down and never left overnight at a client's facility, a successful attack through this path is unlikely to occur.

## 5.4 Ignored Issues

During the course of this effort several areas not addressed by the tools included with the consultant's "kit" were uncovered. Rather than include them in the self-assessment and extend its scope these issues were put aside and are addressed in [Appendix C](#) as recommendations for future consideration.

## 5.5 Review of the Process

The self-assessment process provided in this document is straightforward and requires about two hours of a consultant's time. Although it is absolutely not comprehensive, it provides a field check on the state of the engineered image originally installed on the laptop and indicates whether currently recommended patches, hotfixes and service packs have been applied, and whether any significant problems are present.

The fundamental question as to whether this minimal level of assessment is sufficient or whether a more comprehensive assessment is required is not addressed. While the literature would suggest that a more comprehensive assessment, examining and/or verifying whether all of the known vulnerabilities in the operating system and Company installed tools have been addressed, I believe such a program could not be reliably carried out in the field. The push-back, primarily in the form of non-compliance, would be overwhelming. That is not to say that a long-term program of educating consultants on the importance of stricter vigilance cannot be successful. Approaching the problem by incrementally raising awareness coupled with the introduction of tools that assist the consultant in achieving the Company's desire to protect Company assets, will be much more effective than the current poster campaigns exhorting the consultants to "be careful." Nonetheless, the self-assessment process is a good first step.

The process was strengthened by Bob Grill's review. As a consequence, four additional tests addressing three areas, i.e., passwords, firewall and antivirus, were added as stimulus response tests.

## 5.6 Conclusion

Criteria culled from the trade press and from personal experience were reviewed against the Company Policy and a set of risks of loss was identified. The risks were then examined to determine means by which they could be minimized. The means were reviewed to identify steps a non-expert computer-aware consultant could be expected to successfully complete to ensure that the originally installed security of his laptops had not diminished. These steps were organized into a self-assessment process and the process was applied to one example laptop. Problems identified in the assessment were reviewed and judgment was applied to determine whether the problems constituted an unacceptable

increase in risk of loss. In this one instance, it appears that any increased risk has been acceptably offset by increased mitigation effort and the laptop passes the test.

Given that the individuals conducting the assessment are essentially untrained in the skills necessary to knowledgeably audit their laptop's security in the absence of the checklist above, the question to be answered remains, "Is this process better than what is in place now?" More to the point, "Is this process better than nothing at all?" To that question I believe this document argues affirmatively. Based on that conclusion, the process defined above is recommended for deployment throughout the consulting organization.

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

## Appendix A - Use of Electronic Communication Systems and Media Management Policy (amended for Consulting Group)

### 1. Policy

- 1.1** It is the policy of the Company to ensure that company owned, leased or sponsored electronic communication media, as well as all supporting systems and all data stored or transmitted on them are utilized by Users (as defined below) in a professional and responsible manner, with proper security measures, for the conduct of Company business. *"Use in the conduct of Company business"* shall be construed in a broad sense to include responsible personal use incidental to travel, training, teleworking/telecommuting and the efficient conduct of Company's business. All use of Company's electronic communication media shall be in strict accordance with all provisions of this policy.

### 2. Applicability

- 2.1** All employees, subcontractors, consultants, business partners, and vendors who utilize Company's electronic communication media (herein collectively referred to as "User's").
- 2.2** In the case of client-provided equipment or systems at client sites, the client's respective policies supersede this policy only where any direct conflict exists. Otherwise, this policy remains in effect and co-exists with the client's policies.
- 2.3** This policy will apply to Users on a global basis. However, if any specific provision directly conflicts with applicable country law, regulation or labor agreement, the relevant law, regulation or labor agreement will supersede that section or provision. The remainder of this policy will remain in effect.

### 3. Definitions

- 3.1 Electronic communication media** include, but are not limited to, e-mail; Lotus Notes; the Internet/WWW; intranet; electronic portals; facsimile; telephone; cell phones; voice mail; and other company-supported computing and communication resources for access to and use of internal and/or external host resources and public networks, as well as storage media. The types of media covered in this policy may expand over time as new technology emerges.

### 4. Use of Electronic Communication Media

- 4.1** Electronic communication media and their supporting systems are business tools for Company business purposes. All communications sent over these systems will be considered to be business or work-related communications and subject to Section 5 below (Privacy).
- 4.2** Personal use of electronic communication media is discouraged. Company, however, recognizes that some personal use will occur that is consistent with the efficient conduct of Company business. Nevertheless, such use should be kept to a minimum. Unlawful or inappropriate use of these media, including excessive and irresponsible personal use, is prohibited.

**4.3** Users are strictly prohibited from utilizing electronic communication media to send, peruse, store, transmit, or further distribute information, whether audio, verbal or visual, that may be considered offensive or disruptive. Offensive or disruptive information includes, but is not limited to, the following:

- a. pornography;
- b. obscene, vulgar or profane content;
- c. sexual comments or images;
- d. derogatory or defamatory content, (including jokes, cartoons and gossip) especially those based on race, color, religious creed, national origin, citizenship, marital status, sex, age, disability and U.S. Veteran status;
- e. chain letters;
- f. personal broadcast messages;
- g. religious proselytizing; and/or
- h. partisan political purposes.

In addition, offensive and disruptive information will include any act, behavior or dissemination of information that is prohibited under the laws of the particular jurisdiction.

**4.4** Users are prohibited from the use of electronic communication media in any manner that violates Company policies, including its policies regarding distribution/solicitation, discrimination or sexual harassment.

**4.5** Unauthorized disclosure of Company, client or business partner proprietary or confidential information via electronic communication media is strictly prohibited. Copyrighted materials, trade secrets, proprietary financial and similar information shall not be sent or solicited for receipt without prior and appropriate authorization.

**4.6** U. S. government-restricted data or classified information (usually delineated by all capital letters) must not be contained within or transmitted over electronic communication media under any circumstances.

**4.7** Misrepresenting, obscuring, suppressing or replacing a User's identity, or using another person's identification and/or password on electronic communication media is strictly prohibited. The User name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

**4.8** Sending or forwarding of electronic mail messages to an extensive number of addresses external to Company's domain is prohibited unless written permission from a business unit Vice President has been obtained in advance. In addition, extensive sending or forwarding of non-business electronic mail within Company's domain is prohibited.

## **5. Privacy**

**5.1** In accordance with Section 6 below, and given the large number of publicly accessible systems that much of Company's electronic mail traverses, there should be no expectation of electronic communication media privacy on the part of the User. Users should be cognizant at all times that electronic media messages are public messages, typically accessible not only by Company but also by any number of other entities at any time. Users also should be aware that files or messages that the User has deleted may be stored elsewhere and are not necessarily erased from the network.

## **6. Monitoring of Electronic Communication Media Systems**

**6.1** In order to maximize employee productivity, perform system maintenance, protect the company against theft of proprietary information, prevent employee malfeasance and system misuse, investigate unlawful or prohibited actions, respond to discovery requests in litigation and investigations, monitor employee job performance and, in general, protect the company's business interests, Company reserves the right to monitor these systems at any time. Company will exercise this right to monitor in a judicious manner.

**6.2** System administrators, human resources representatives and members of the legal department and their agents are authorized to monitor and access electronic communication media systems as directed by the Corporate Chief Technology Officer, the Corporate Vice President, Human Resources, or the General Counsel, or their designee(s). Company reserves the right to retrieve, read, copy, download, and save any information composed, sent, received, or stored over these systems, regardless of whether the system is being used at the work site or at any remote location, including the User's home. While Company reserves the right through its authorized personnel to retrieve, read, copy, download and save any electronic information transmitted over any of Company's systems or equipment, such information otherwise should be treated as confidential by Users and accessed only by the intended recipients.

**6.3** In order to prevent unintended disclosure, extreme care should be exercised to prevent the missending or interception of data. In addition, Users should minimize storage of confidential or proprietary data to prevent unintended disclosure.

**6.4** It is not Company's policy to allow outside auditors, governmental regulators or any external third party access to these systems unless legally required to do so. Unintended disclosure may result in the discovery and production of confidential or proprietary data in legal proceedings. However, using encryption and marking electronically transmitted messages as company confidential or as privileged for the advice of counsel and only providing access through counsel to those having an absolute need to know, may strengthen the company's ability to protect against the disclosure of confidential or proprietary data to third parties during legal proceedings.

**6.5** Under the Electronic Communications Privacy Act, it is a criminal act to intercept electronic communications not addressed to you without authorization to do so. (See 18 United States Code Amendment 2701 et seq.)

**6.6** Unauthorized electronic snooping including, but not limited to, network probing or cracking, by any User is prohibited.

## **7. Security and Integrity of Electronic Communication Media Systems**

**7.1** To protect the integrity of the information transmitted through these systems, Users should send confidential or proprietary messages only to the necessary recipients and must mark those messages as company confidential and/or company proprietary. Such messages should be encrypted, both prior to sending and prior to storage. Users must not leave confidential information on their screens when they leave their workstations. Storage should be limited to the shortest practical or legally required time period.

**7.2** To protect against the unauthorized use of these systems, a form of strong password protection must be used. Strong passwords contain a combination of alphabetic



characters plus symbols and numbers and should not be found in any dictionary, including foreign dictionaries. Strong passwords must:

- have a minimum of eight (8), but no more than sixteen (16) characters
- have at least two (2) alphabetic characters (a-z, A-Z)
- have at least two (2) numerical characters (0-9)
- and have at least one (1) "special" character, such as the following:  
(~ ` ! @ # \$ % ^ & \* ( ) \_ - + = , . / \ { } [ ] ; : < > ? " ' )

The use of such strong passwords, however, should not create an expectation of privacy on the part of the User. Users should also be aware that Company has the ability and reserves the right to override passwords.

**7.3** To protect the integrity and security of these systems, Users are prohibited from disrupting software or system performance or intentionally introducing viruses and must comply with all Company instructions on preventing the introduction of viruses. The development, production, transmission or forwarding of computer viruses, denial of service agents, or any other processes that are designed to interrupt or otherwise negatively impact electronic communication or communications systems is strictly prohibited.

**7.4** Legal downloading of software or files from public sources is permitted for conducting Company business. However, shareware is licensed material and must be paid for in accordance with the corresponding license agreement. Unlicensed material may not be used in conjunction with Company's electronic communication media. In addition, reasonable measures, including, but not limited to virus scanning, must be taken immediately after downloading files and prior to launching or installing software to ensure that virus-infected software is not introduced into Company systems.

**7.5** All computer security events (actual or attempted) such as break-ins, data tampering, virus outbreaks, and inappropriate or unauthorized use of electronic communication media must be reported immediately to the Computer Emergency Response Coordination Center (CERCC), at the following e-mail address: [CERCC@Company.com](mailto:CERCC@Company.com).

**7.6** All Company directories and address books are Company Proprietary. They must at all times reside within the Company firewall. Under limited circumstances non-Company individuals or entities may be granted access to portions of Company's Address Book. Small and appropriate portions of the Company Mail Address Book may be provided to clients who have a need to exchange mail with Company staff in the conduct of Company business. Company's Corporate Chief Technology Officer must formally approve each such instance in advance.

**7.7** Any computer equipment received by user, such as laptop, accessories, and other peripherals are Company property and should be properly cared for. Depending on the severity and the cause, user can be held responsible for damages that result from misuse or abuse.

**7.8** (Added for Consulting Group) User who is assigned a computer can use the computer for business use. Any personal use is against Company policy, unless prior approval by management or an internal systems administrator.

**7.9** (Added for Consulting Group) User is responsible for adhering to the Company Software Licensing Policy. Any additional software installed on this laptop must be properly licensed or can be removed, at will, by an internal systems administrator.

**7.10** (Added for Consulting Group) Users responsible for systems running WinNT or Win2000 OS are not allowed to make any changes to the local administrator account on this machine AND are not allowed to change the domain to which the machine is registered without first contacting a Company intranet systems administrator. Doing so can make your machine incapable of use and a new image may be required.

## **8. Violations of the Policy**

**8.1** Any employee who engages in behavior prohibited by this policy or who fails to protect the integrity and security of any electronic communication media, shall be in violation of Human Resources Management Policy on **Employee Conduct** and shall be subject to appropriate disciplinary action, up to and including termination of employment.

## **9. Exceptions**

**9.1** Exceptions to this policy shall be authorized only with the written approval of the Corporate Vice President of Human Resources (in coordination with the General Counsel and Corporate Chief Technology Officer).

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

## Appendix B – ZoneAlarm Log

Type	Date	Time	Source	Port	Destination	Port	Transport	Severity
FWIN	3/29/2002	1:33:16 PM	64.164.113.219	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/29/2002	12:02:16 PM	64.164.113.219	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/29/2002	10:51:58 AM	64.164.113.219	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/27/2002	4:00:36 PM	206.171.158.131	0	172.16.1.34	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/27/2002	4:00:22 PM	144.232.9.174	0	172.16.1.34	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/27/2002	4:00:02 PM	63.211.54.85	0	172.16.1.34	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/27/2002	4:00:00 PM	216.140.8.193	0	172.16.1.34	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/27/2002	3:59:54 PM	216.140.8.18	0	172.16.1.34	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/27/2002	1:38:32 PM	64.164.113.219	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/27/2002	8:48:18 AM	64.164.112.89	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/27/2002	2:47:20 AM	64.164.112.89	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/27/2002	1:04:28 AM	172.16.0.1	0	172.16.1.34	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/25/2002	6:04:56 PM	64.164.114.105	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/25/2002	5:03:06 PM	64.164.114.105	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/25/2002	2:16:22 PM	64.164.114.105	0	172.16.1.34	0	ICMP (type:3/subtype:4)	Harmless
FWIN	3/25/2002	11:27:40 AM	204.177.254.236	0	63.59.135.162	0	ICMP (type:3/subtype:9)	Harmless
FWIN	3/25/2002	11:17:58 AM	4.24.6.22	0	63.59.135.162	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/25/2002	11:14:56 AM	63.59.13.10	3007	63.59.135.162	80	TCP (flags:S)	Harmless
FWIN	3/25/2002	10:52:24 AM	63.227.234.170	1622	63.59.135.162	80	TCP (flags:S)	Harmless
FWIN	3/25/2002	1:14:48 AM	204.146.167.83	0	63.59.135.240	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/24/2002	9:14:48 PM	204.146.167.71	0	63.59.135.201	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/24/2002	9:14:48 PM	204.146.167.83	0	63.59.135.201	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/24/2002	8:07:58 PM	68.38.67.35	4835	63.59.135.221	12345	TCP (flags:S)	Trojan
FWIN	3/24/2002	7:34:04 PM	204.146.167.83	0	63.59.135.221	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/24/2002	7:33:08 PM	204.146.167.71	0	63.59.135.221	0	ICMP (type:8/subtype:0)	Harmless
FWROUTE	3/24/2002	6:11:00 PM	172.16.0.1	0	172.16.1.34	0	ICMP (type:8/subtype:0)	

FWIN	3/24/2002	8:33:38 AM	216.125.196.5	2732	63.59.135.140	111	TCP (flags:S)	Scan
FWIN	3/24/2002	12:54:00 AM	61.253.4.8	2756	63.59.135.140	111	TCP (flags:S)	Scan
FWIN	3/23/2002	10:56:30 PM	212.216.205.199	22	63.59.135.140	22	TCP (flags:S)	Scan
FWIN	3/23/2002	9:34:54 PM	63.59.92.32	1401	63.59.135.140	80	TCP (flags:S)	Harmless
FWIN	3/23/2002	9:25:36 PM	63.59.92.32	2717	63.59.135.140	80	TCP (flags:S)	Harmless
FWIN	3/23/2002	9:19:58 PM	63.59.92.32	3986	63.59.135.140	80	TCP (flags:S)	Harmless
FWIN	3/23/2002	8:59:26 PM	63.59.92.32	2778	63.59.135.140	80	TCP (flags:S)	Harmless
FWIN	3/23/2002	8:54:48 PM	61.141.208.78	3439	63.59.135.140	111	TCP (flags:S)	Scan
FWIN	3/23/2002	6:48:14 PM	209.202.218.112	80	63.59.135.140	58731	TCP (flags:S)	Unknown
FWIN	3/23/2002	6:47:58 PM	209.202.218.125	80	63.59.135.140	24398	TCP (flags:S)	Unknown
FWIN	3/23/2002	6:47:50 PM	209.202.218.122	80	63.59.135.140	21946	TCP (flags:S)	Unknown
FWIN	3/23/2002	6:36:48 PM	61.182.50.241	3402	63.59.135.140	111	TCP (flags:S)	Scan
FWIN	3/23/2002	2:52:46 PM	61.211.225.15	3729	63.59.135.121	111	TCP (flags:S)	Scan
FWIN	3/23/2002	12:36:58 PM	137.53.85.170	50816	63.59.135.121	6346	TCP (flags:S)	Harmless
FWIN	3/23/2002	10:42:30 AM	61.218.151.228	4309	63.59.135.121	111	TCP (flags:S)	Scan
FWIN	3/23/2002	4:29:14 AM	63.205.53.43	2541	63.59.135.121	80	TCP (flags:S)	Harmless
FWIN	3/23/2002	3:50:40 AM	64.221.92.236	54376	63.59.135.121	515	TCP (flags:S)	Scan
FWIN	3/22/2002	2:56:50 PM	172.152.18.10	3126	63.59.135.78	27374	TCP (flags:S)	Trojan
FWIN	3/22/2002	2:46:04 PM	202.234.170.131	4872	63.59.135.78	111	TCP (flags:S)	Scan
FWOUT	3/22/2002	2:17:36 PM	63.59.135.78	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/22/2002	1:16:40 PM	63.59.135.126	1140	63.59.135.206	12345	TCP (flags:S)	Trojan
FWIN	3/22/2002	12:08:54 PM	204.146.167.71	0	63.59.135.206	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/22/2002	12:00:28 PM	204.146.167.83	0	63.59.135.206	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/22/2002	10:23:12 AM	64.52.49.98	41275	63.59.135.206	38293	UDP	Unknown
FWIN	3/22/2002	5:39:24 AM	202.109.72.29	1733	63.59.135.206	111	TCP (flags:S)	Scan
FWIN	3/22/2002	5:17:50 AM	216.175.67.115	4668	63.59.135.206	1080	TCP (flags:S)	Trojan
FWIN	3/22/2002	4:42:32 AM	63.229.177.161	2326	63.59.135.206	111	TCP (flags:S)	Scan
FWIN	3/22/2002	4:26:46 AM	65.168.20.2	1904	63.59.135.206	21	TCP (flags:S)	Attack
FWIN	3/22/2002	3:21:10 AM	63.175.115.47	3678	63.59.135.206	80	TCP (flags:S)	Harmless
FWIN	3/22/2002	1:16:34 AM	209.179.41.137	4858	63.59.135.206	31337	UDP	Trojan
FWIN	3/22/2002	1:06:52 AM	211.144.23.2	1320	63.59.135.206	111	TCP (flags:S)	Scan

FWIN	3/22/2002	12:48:22 AM	66.76.49.160	4703	63.59.135.206	27374	TCP (flags:S)	Trojan
FWOUT	3/21/2002	10:29:40 PM	63.59.135.206	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWOUT	3/21/2002	10:23:20 PM	63.59.135.171	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWOUT	3/21/2002	10:22:24 PM	172.16.1.34	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/21/2002	10:22:22 PM	172.192.138.180	4333	63.59.135.99	27374	TCP (flags:S)	Trojan
FWOUT	3/21/2002	9:04:26 PM	172.16.1.34	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/21/2002	8:04:24 PM	209.179.41.137	4202	63.59.135.57	31337	UDP	Trojan
FWOUT	3/21/2002	7:47:54 PM	63.59.135.57	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWOUT	3/21/2002	7:47:52 PM	172.16.1.34	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/21/2002	3:05:56 PM	140.186.45.15	80	63.59.135.205	17024	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:56 PM	140.186.45.15	80	63.59.135.205	15064	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:56 PM	140.186.45.14	80	63.59.135.205	19296	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:52 PM	140.186.45.15	80	63.59.135.205	18084	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:52 PM	140.186.45.15	80	63.59.135.205	14823	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:50 PM	140.186.45.15	80	63.59.135.205	6137	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:50 PM	140.186.45.15	80	63.59.135.205	6128	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:05:48 PM	140.186.45.15	80	63.59.135.205	11170	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:56 PM	140.186.45.15	80	63.59.135.205	15064	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:56 PM	140.186.45.15	80	63.59.135.205	17024	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:52 PM	140.186.45.15	80	63.59.135.205	18084	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:52 PM	140.186.45.15	80	63.59.135.205	14823	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:50 PM	140.186.45.15	80	63.59.135.205	6137	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:50 PM	140.186.45.15	80	63.59.135.205	6128	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:48 PM	140.186.45.15	80	63.59.135.205	11170	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:02 PM	140.186.45.15	80	63.59.135.205	15064	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:02 PM	140.186.45.14	80	63.59.135.205	19296	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:03:02 PM	140.186.45.15	80	63.59.135.205	17024	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:02:58 PM	140.186.45.15	80	63.59.135.205	18084	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:02:58 PM	140.186.45.15	80	63.59.135.205	14823	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:02:56 PM	140.186.45.15	80	63.59.135.205	6128	TCP (flags:S)	Unknown
FWIN	3/21/2002	3:02:56 PM	140.186.45.15	80	63.59.135.205	6137	TCP (flags:S)	Unknown

FWIN	3/21/2002	3:02:54 PM	140.186.45.15	80	63.59.135.205	11170	TCP (flags:S)	Unknown
FWIN	3/21/2002	1:11:10 PM	206.132.113.125	0	63.59.135.205	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/21/2002	12:33:16 PM	20.8.10.191	1352	63.59.135.205	4343	TCP (flags:S)	Unknown
FWIN	3/21/2002	11:14:42 AM	61.145.136.97	0	63.59.135.205	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/21/2002	10:56:14 AM	142.177.71.111	2837	63.59.135.205	1214	TCP (flags:S)	Harmless
FWIN	3/21/2002	10:51:02 AM	24.129.37.78	22	63.59.135.205	22	TCP (flags:S)	Scan
FWIN	3/21/2002	10:43:14 AM	142.177.71.111	2547	63.59.135.205	1214	TCP (flags:S)	Harmless
FWIN	3/21/2002	9:27:14 AM	61.8.229.50	55753	63.59.135.205	21	TCP (flags:S)	Attack
FWIN	3/21/2002	8:47:54 AM	65.42.228.137	1025	63.59.135.205	137	UDP	Attack
FWIN	3/21/2002	8:06:00 AM	209.10.50.213	80	63.59.135.205	20100	TCP (flags:S)	Unknown
FWIN	3/21/2002	5:49:18 AM	217.13.104.34	1041	63.59.135.205	137	UDP	Attack
FWIN	3/21/2002	4:06:28 AM	199.104.108.199	2787	63.59.135.205	21	TCP (flags:S)	Attack
FWIN	3/21/2002	3:59:04 AM	202.109.72.29	3540	63.59.135.205	111	TCP (flags:S)	Scan
FWIN	3/20/2002	8:00:00 PM	194.109.127.64	80	63.59.135.205	13984	TCP (flags:S)	Unknown
FWIN	3/20/2002	2:41:12 PM	211.251.148.1	3819	63.59.135.122	111	TCP (flags:S)	Scan
FWIN	3/20/2002	2:20:36 PM	208.45.244.9	4667	63.59.135.122	80	TCP (flags:S)	Harmless
FWIN	3/20/2002	12:11:12 PM	206.64.118.87	47821	63.59.135.1	33468	UDP	Unknown
FWIN	3/20/2002	12:11:10 PM	206.64.118.87	47821	63.59.135.1	33467	UDP	Unknown
FWIN	3/20/2002	12:11:06 PM	206.64.118.87	47821	63.59.135.1	33466	UDP	Unknown
FWIN	3/20/2002	12:11:02 PM	206.64.118.87	47821	63.59.135.1	33465	UDP	Unknown
FWIN	3/20/2002	10:13:02 AM	206.64.118.87	42888	63.59.135.1	33468	UDP	Unknown
FWIN	3/20/2002	10:12:58 AM	206.64.118.87	42888	63.59.135.1	33467	UDP	Unknown
FWIN	3/20/2002	10:12:56 AM	206.64.118.87	42888	63.59.135.1	33466	UDP	Unknown
FWIN	3/20/2002	10:12:50 AM	206.64.118.87	42888	63.59.135.1	33465	UDP	Unknown
FWIN	3/20/2002	9:39:14 AM	10.112.1.1	80	63.59.135.1	4801	TCP (flags:S)	Unknown
FWIN	3/20/2002	9:38:40 AM	12.125.101.102	0	63.59.135.1	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/20/2002	9:38:34 AM	12.125.101.106	0	63.59.135.1	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/20/2002	8:11:16 AM	206.64.118.87	37973	63.59.135.1	33468	UDP	Unknown
FWIN	3/20/2002	8:11:14 AM	206.64.118.87	37973	63.59.135.1	33467	UDP	Unknown
FWIN	3/20/2002	8:11:12 AM	206.64.118.87	37973	63.59.135.1	33466	UDP	Unknown
FWIN	3/20/2002	8:11:04 AM	206.64.118.87	37973	63.59.135.1	33465	UDP	Unknown

FWIN	3/19/2002	9:36:12 PM	61.33.232.2	21	63.59.135.101	21	TCP (flags:S)	Attack
FWIN	3/19/2002	9:01:18 PM	217.136.131.33	3625	63.59.135.101	21	TCP (flags:S)	Attack
FWIN	3/19/2002	6:25:06 PM	152.63.48.30	0	63.59.135.205	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/19/2002	6:25:06 PM	152.63.48.30	0	63.59.135.205	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/19/2002	6:21:56 PM	208.39.140.9	0	63.59.135.205	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/19/2002	6:21:56 PM	208.39.140.9	0	63.59.135.205	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/19/2002	3:57:28 PM	216.175.102.59	1027	63.59.135.205	137	UDP	Attack
FWIN	3/19/2002	3:57:28 PM	216.175.102.59	1027	63.59.135.205	137	UDP	Attack
FWIN	3/19/2002	3:55:12 PM	202.155.107.132	1028	63.59.135.205	137	UDP	Attack
FWIN	3/19/2002	3:55:12 PM	202.155.107.132	1028	63.59.135.205	137	UDP	Attack
FWIN	3/19/2002	10:47:20 AM	204.186.114.237	137	63.59.135.44	137	UDP	Attack
FWIN	3/19/2002	6:58:02 AM	65.202.57.10	22	63.59.135.44	22	TCP (flags:S)	Scan
FWIN	3/19/2002	4:09:44 AM	172.176.17.230	4035	63.59.135.44	27374	TCP (flags:S)	Trojan
FWIN	3/19/2002	3:30:34 AM	218.12.108.7	63236	63.59.135.44	80	TCP (flags:S)	Harmless
FWIN	3/19/2002	2:22:18 AM	213.198.165.49	2431	63.59.135.44	80	TCP (flags:S)	Harmless
FWIN	3/18/2002	10:33:20 PM	209.247.137.43	1348	63.59.135.44	6346	TCP (flags:S)	Harmless
FWIN	3/18/2002	6:53:08 PM	205.151.61.77	3141	63.59.135.44	80	TCP (flags:S)	Harmless
FWIN	3/18/2002	3:22:18 PM	10.1.50.6	0	63.59.135.44	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/18/2002	12:59:58 PM	213.186.70.10	2257	63.59.135.44	22	TCP (flags:S)	Scan
FWIN	3/18/2002	12:30:58 PM	61.10.25.110	2926	63.59.135.44	111	TCP (flags:S)	Scan
FWIN	3/18/2002	11:02:28 AM	61.134.23.163	4635	63.59.135.39	515	TCP (flags:S)	Scan
FWIN	3/18/2002	10:45:32 AM	62.229.90.210	3538	63.59.135.39	80	TCP (flags:S)	Harmless
FWIN	3/18/2002	10:07:36 AM	216.154.238.10	4642	63.59.135.39	80	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:37:50 AM	193.251.74.60	1301	166.72.254.132	80	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:12:46 AM	165.87.194.246	41533	166.72.254.132	113	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:12:46 AM	165.87.194.246	41534	166.72.254.132	113	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:12:46 AM	165.87.194.246	41532	166.72.254.132	113	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:10:34 AM	165.87.194.246	51076	166.72.254.132	113	TCP (flags:S)	Harmless
FWIN	3/18/2002	8:10:32 AM	165.87.194.246	51071	166.72.254.132	113	TCP (flags:S)	Harmless
FWIN	3/18/2002	1:28:42 AM	147.208.130.207	80	63.59.135.204	8467	TCP (flags:S)	Unknown
FWIN	3/18/2002	1:27:20 AM	147.208.130.207	80	63.59.135.204	8467	TCP (flags:S)	Unknown

FWOUT	3/18/2002	1:13:42 AM	63.59.135.204	1871	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1868	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1863	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1867	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1869	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1870	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:40 AM	63.59.135.204	1864	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:36 AM	63.59.135.204	1886	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:34 AM	63.59.135.204	1885	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:34 AM	63.59.135.204	1884	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:34 AM	63.59.135.204	1883	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:34 AM	63.59.135.204	1881	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:34 AM	63.59.135.204	1880	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:32 AM	63.59.135.204	1876	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:32 AM	63.59.135.204	1879	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:32 AM	63.59.135.204	1877	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:32 AM	63.59.135.204	1889	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1872	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1873	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1887	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1871	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1875	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:30 AM	63.59.135.204	1890	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1889	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1863	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1888	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1864	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1881	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1868	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1869	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1870	192.149.252.22	43	TCP (flags:S)	



FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1880	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:28 AM	63.59.135.204	1867	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1886	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1884	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1885	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1877	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1887	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1879	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:26 AM	63.59.135.204	1876	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1881	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1877	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1872	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1879	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1873	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1874	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1875	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:24 AM	63.59.135.204	1880	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:22 AM	63.59.135.204	1874	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:22 AM	63.59.135.204	1875	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:22 AM	63.59.135.204	1876	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:22 AM	63.59.135.204	1863	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1869	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1873	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1872	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1870	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1868	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:20 AM	63.59.135.204	1871	192.149.252.22	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:18 AM	63.59.135.204	1863	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:18 AM	63.59.135.204	1864	63.146.182.182	43	TCP (flags:S)	
FWOUT	3/18/2002	1:13:18 AM	63.59.135.204	1867	192.149.252.22	43	TCP (flags:S)	
FWIN	3/18/2002	12:30:16 AM	61.30.144.135	4061	63.59.135.204	111	TCP (flags:S)	Scan

FWIN	3/17/2002	9:13:28 PM	202.133.132.30	1468	63.59.135.204	137	UDP	Attack
FWIN	3/17/2002	9:04:06 PM	67.32.195.252	1040	63.59.135.204	137	UDP	Attack
FWIN	3/17/2002	7:33:44 PM	211.174.51.21	4012	63.59.135.204	53	TCP (flags:S)	Attack
FWIN	3/17/2002	6:33:10 PM	61.9.80.171	1029	63.59.135.204	137	UDP	Attack
FWIN	3/17/2002	6:23:04 PM	64.52.49.98	43013	63.59.135.204	38293	UDP	Unknown
FWIN	3/17/2002	4:01:34 PM	208.16.210.18	137	63.59.135.221	137	UDP	Attack
FWIN	3/17/2002	1:07:06 PM	200.193.224.35	3466	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	1:01:30 PM	206.46.188.41	80	63.59.135.188	20616	TCP (flags:S)	Unknown
FWIN	3/17/2002	1:01:28 PM	200.193.224.35	3325	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	1:01:20 PM	206.46.188.40	80	63.59.135.188	17461	TCP (flags:S)	Unknown
FWIN	3/17/2002	1:00:52 PM	206.46.188.39	80	63.59.135.188	4528	TCP (flags:S)	Unknown
FWIN	3/17/2002	12:54:10 PM	200.193.224.35	3163	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:48:42 PM	200.193.224.35	3054	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:42:14 PM	200.193.224.35	2950	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:41:40 PM	147.208.183.104	80	63.59.135.188	23665	TCP (flags:S)	Unknown
FWIN	3/17/2002	12:35:08 PM	200.193.224.35	2846	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:28:42 PM	200.193.224.35	2731	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:21:46 PM	200.193.224.35	2582	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:16:08 PM	200.193.224.35	2474	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:10:02 PM	200.193.224.35	2359	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	12:03:56 PM	200.193.224.35	2266	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:57:58 AM	200.193.224.35	2180	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:51:46 AM	200.193.224.35	2071	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:45:20 AM	200.193.224.35	1936	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:42:34 AM	216.200.14.240	0	63.59.135.188	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/17/2002	11:39:04 AM	200.193.224.35	1803	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:32:56 AM	200.193.224.35	1640	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:26:42 AM	200.193.224.35	1517	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:20:36 AM	200.193.224.35	1406	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:14:16 AM	200.193.224.35	1289	63.59.135.188	1214	TCP (flags:S)	Harmless
FWIN	3/17/2002	11:08:00 AM	200.193.224.35	1158	63.59.135.188	1214	TCP (flags:S)	Harmless

FWIN	3/17/2002	10:54:36 AM	24.103.152.145	1757	63.59.135.188	6366	TCP (flags:S)	Unknown
FWIN	3/17/2002	10:48:04 AM	67.235.47.148	3084	63.59.135.188	137	UDP	Attack
FWIN	3/16/2002	10:10:34 PM	216.200.14.240	0	63.59.135.11	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/16/2002	10:37:50 AM	66.146.40.143	4329	63.59.135.9	31337	UDP	Trojan
FWIN	3/16/2002	5:44:16 AM	218.13.13.71	2637	63.59.135.9	80	TCP (flags:S)	Harmless
FWIN	3/16/2002	4:33:20 AM	61.144.181.37	0	63.59.135.9	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/16/2002	2:48:22 AM	211.18.250.93	21	63.59.135.9	21	TCP (flags:S)	Attack
FWIN	3/15/2002	9:08:26 PM	172.128.157.2	3397	63.59.135.9	1080	TCP (flags:S)	Trojan
FWIN	3/15/2002	5:21:34 PM	218.21.77.128	4980	63.59.135.9	80	TCP (flags:S)	Harmless
FWIN	3/15/2002	3:48:02 PM	210.52.77.19	1246	63.59.135.9	111	TCP (flags:S)	Scan
FWOUT	3/15/2002	11:12:14 AM	172.16.1.34	1030	172.16.1.33	139	TCP (flags:S)	
FWIN	3/15/2002	11:11:26 AM	172.16.0.1	0	172.16.1.34	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/15/2002	10:18:36 AM	212.98.68.51	21	63.59.135.14	21	TCP (flags:S)	Attack
FWIN	3/15/2002	10:10:48 AM	20.8.10.191	1352	63.59.135.14	4362	TCP (flags:S)	Unknown
FWIN	3/15/2002	9:39:20 AM	12.27.150.4	0	63.59.135.14	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/15/2002	7:58:58 AM	162.33.235.25	4962	63.59.135.14	80	TCP (flags:S)	Harmless
FWIN	3/15/2002	1:52:02 AM	61.141.208.78	1999	63.59.135.14	111	TCP (flags:S)	Scan
FWIN	3/14/2002	8:52:18 PM	208.17.163.18	137	63.59.135.14	137	UDP	Attack
FWIN	3/14/2002	8:52:18 PM	208.17.163.100	137	63.59.135.14	137	UDP	Attack
FWROUTE	3/14/2002	8:49:02 PM	63.59.135.14	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/14/2002	8:13:54 PM	65.194.17.150	2200	63.59.135.196	80	TCP (flags:S)	Harmless
FWIN	3/14/2002	3:57:44 PM	210.93.206.19	4623	63.59.135.196	111	TCP (flags:S)	Scan
FWROUTE	3/14/2002	2:29:22 PM	63.59.135.196	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/14/2002	2:14:16 PM	65.129.52.31	4073	63.59.135.82	1214	TCP (flags:S)	Harmless
FWOUT	3/14/2002	2:13:06 PM	63.59.135.82	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/14/2002	9:20:54 AM	64.52.49.98	53243	63.59.135.56	38293	UDP	Unknown
FWIN	3/14/2002	5:42:48 AM	200.40.198.4	1963	63.59.135.56	22	TCP (flags:S)	Scan
FWIN	3/14/2002	3:24:52 AM	152.149.43.5	54080	63.59.135.56	111	TCP (flags:S)	Scan
FWOUT	3/14/2002	2:44:46 AM	63.59.135.56	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWOUT	3/14/2002	2:44:46 AM	63.59.135.56	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/14/2002	2:23:18 AM	152.63.48.26	0	63.59.135.56	0	ICMP (type:3/subtype:1)	Harmless

FWIN	3/14/2002	2:10:02 AM	216.200.14.231	0	63.59.135.56	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/14/2002	2:01:54 AM	194.108.12.45	4993	63.59.135.56	53	TCP (flags:S)	Attack
FWIN	3/14/2002	1:42:58 AM	63.225.208.105	2343	63.59.135.56	161	UDP	Harmless
FWIN	3/14/2002	1:25:54 AM	218.27.17.2	4236	63.59.135.56	80	TCP (flags:S)	Harmless
FWIN	3/14/2002	12:35:56 AM	134.126.34.149	2482	63.59.135.56	80	TCP (flags:S)	Harmless
FWIN	3/13/2002	10:50:18 PM	202.101.10.231	1402	63.59.135.56	80	TCP (flags:S)	Harmless
FWIN	3/13/2002	8:09:30 PM	66.45.5.31	80	63.59.135.56	3156	TCP (flags:S)	Unknown
FWIN	3/13/2002	6:26:54 PM	216.33.9.126	80	63.59.135.56	2709	TCP (flags:S)	Unknown
FWIN	3/13/2002	1:53:06 PM	63.25.191.47	4330	63.59.135.56	80	TCP (flags:S)	Harmless
FWIN	3/13/2002	1:19:46 AM	64.245.51.178	3140	63.59.135.9	21	TCP (flags:S)	Attack
FWIN	3/13/2002	12:50:26 AM	61.30.144.135	4587	63.59.135.9	111	TCP (flags:S)	Scan
FWIN	3/12/2002	3:59:10 PM	203.251.225.30	3943	63.59.135.166	80	TCP (flags:S)	Harmless
FWIN	3/12/2002	3:40:30 PM	194.106.126.51	4284	63.59.135.166	80	TCP (flags:S)	Harmless
FWIN	3/12/2002	12:31:12 PM	172.143.148.161	2225	63.59.135.166	1214	TCP (flags:S)	Harmless
FWIN	3/12/2002	12:03:20 PM	172.130.251.192	3746	63.59.135.166	1214	TCP (flags:S)	Harmless
FWIN	3/12/2002	12:02:12 PM	64.133.109.229	21	63.59.135.166	21	TCP (flags:S)	Attack
FWIN	3/12/2002	10:01:48 AM	206.196.101.194	3545	63.59.135.166	80	TCP (flags:S)	Harmless
FWIN	3/12/2002	6:26:12 AM	218.2.178.40	0	63.59.135.166	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/12/2002	1:21:16 AM	64.52.49.98	36421	63.59.135.166	38293	UDP	Unknown
FWIN	3/11/2002	2:20:34 PM	63.198.46.178	1682	63.59.135.127	22	TCP (flags:S)	Scan
FWIN	3/11/2002	8:41:54 AM	212.7.17.119	3696	63.59.135.127	21	TCP (flags:S)	Attack
FWIN	3/11/2002	8:14:30 AM	61.142.73.229	4874	63.59.135.127	80	TCP (flags:S)	Harmless
FWIN	3/11/2002	6:52:42 AM	63.228.146.224	3357	63.59.135.127	80	TCP (flags:S)	Harmless
FWIN	3/11/2002	6:29:06 AM	63.228.146.224	3689	63.59.135.127	80	TCP (flags:S)	Harmless
FWIN	3/11/2002	6:22:22 AM	24.191.65.214	21	63.59.135.127	21	TCP (flags:S)	Attack
FWIN	3/11/2002	5:52:38 AM	68.14.15.230	22	63.59.135.127	22	TCP (flags:S)	Scan
FWIN	3/10/2002	5:08:44 PM	207.64.77.2	1630	63.59.135.47	53	TCP (flags:S)	Attack
FWIN	3/10/2002	4:45:26 PM	210.96.77.61	4423	63.59.135.47	22	TCP (flags:S)	Scan
FWIN	3/10/2002	4:28:34 PM	210.104.143.253	31334	63.59.135.47	80	TCP (flags:S)	Harmless
FWIN	3/10/2002	4:07:14 PM	210.178.12.111	46877	63.59.135.47	111	TCP (flags:S)	Scan
FWIN	3/10/2002	3:17:10 PM	211.159.68.124	1892	63.59.135.47	80	TCP (flags:S)	Harmless

FWIN	3/10/2002	2:24:22 PM	63.197.79.111	65325	63.59.135.47	80	TCP (flags:S)	Harmless
FWIN	3/10/2002	1:24:06 PM	205.152.84.49	4121	63.59.135.47	80	TCP (flags:S)	Harmless
FWIN	3/10/2002	12:34:30 PM	130.67.199.221	1448	63.59.135.47	80	TCP (flags:S)	Harmless
FWIN	3/10/2002	12:08:10 PM	211.196.77.138	4385	63.59.135.47	80	TCP (flags:S)	Harmless
FWIN	3/10/2002	12:00:24 PM	205.188.134.194	81	63.59.135.47	4026	TCP (flags:S)	Unknown
FWIN	3/10/2002	11:22:18 AM	217.136.177.250	3633	63.59.135.47	21	TCP (flags:S)	Attack
FWIN	3/10/2002	11:04:32 AM	216.33.9.28	80	63.59.135.47	3142	TCP (flags:S)	Unknown
FWIN	3/10/2002	3:41:18 AM	66.13.140.90	2876	63.59.135.47	111	TCP (flags:S)	Scan
FWIN	3/9/2002	11:16:48 PM	213.225.71.41	4668	63.59.135.47	111	TCP (flags:S)	Scan
FWIN	3/9/2002	9:20:00 PM	209.86.98.115	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	9:19:54 PM	24.88.153.163	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:57:46 PM	68.7.74.176	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:51:44 PM	213.134.14.162	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:48:22 PM	165.121.194.82	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:46:04 PM	142.59.240.138	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:38:30 PM	24.209.19.15	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:37:14 PM	172.131.209.162	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:35:10 PM	67.200.202.180	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	8:31:38 PM	210.6.9.75	13139	63.59.135.47	13139	UDP	Harmless
FWIN	3/9/2002	5:54:38 PM	152.63.55.113	0	63.59.135.64	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/9/2002	5:52:10 PM	152.63.55.125	0	63.59.135.64	0	ICMP (type:11/subtype:0)	Harmless
FWIN	3/9/2002	5:16:51 PM	80.133.44.164	0	63.59.135.64	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/9/2002	3:48:14 PM	63.225.196.14	0	63.59.135.64	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/9/2002	2:40:02 PM	61.182.251.173	7002	63.59.135.64	4000	UDP	Harmless
FWIN	3/9/2002	1:55:09 PM	210.83.7.164	61451	63.59.135.64	4000	UDP	Harmless
FWIN	3/9/2002	1:55:09 PM	210.83.7.164	62688	63.59.135.64	4003	UDP	Unknown
FWIN	3/9/2002	1:55:09 PM	210.83.7.164	62103	63.59.135.64	4001	UDP	Unknown
FWIN	3/9/2002	1:55:09 PM	210.83.7.164	62104	63.59.135.64	4002	UDP	Unknown
FWIN	3/9/2002	1:41:59 PM	216.129.203.68	3859	63.59.135.64	111	TCP (flags:S)	Scan
FWIN	3/9/2002	12:57:45 PM	67.105.80.70	4008	63.59.135.64	515	TCP (flags:S)	Scan
FWIN	3/9/2002	12:43:39 PM	210.49.82.43	1464	63.59.135.64	53	TCP (flags:S)	Attack

FWIN	3/9/2002	9:36:49 AM	24.201.241.36	1106	63.59.135.64	27374	TCP (flags:S)	Trojan
FWIN	3/9/2002	7:26:22 AM	63.59.255.176	3867	63.59.135.64	80	TCP (flags:S)	Harmless
FWIN	3/9/2002	6:11:56 AM	65.92.244.57	3530	63.59.135.64	27374	TCP (flags:S)	Trojan
FWIN	3/9/2002	6:10:37 AM	64.45.219.202	1032	63.59.135.64	137	UDP	Attack
FWIN	3/9/2002	3:05:54 AM	61.175.218.158	3635	63.59.135.64	80	TCP (flags:S)	Harmless
FWIN	3/9/2002	1:54:09 AM	66.46.61.130	2820	63.59.135.64	53	TCP (flags:S)	Attack
FWIN	3/8/2002	4:25:59 PM	216.129.203.68	2962	63.59.135.42	111	TCP (flags:S)	Scan
FWIN	3/8/2002	3:34:57 PM	65.65.203.105	3519	63.59.135.42	27374	TCP (flags:S)	Trojan
FWIN	3/8/2002	2:21:44 PM	198.80.170.134	137	63.59.135.42	137	UDP	Attack
FWIN	3/8/2002	2:01:05 PM	166.41.247.47	137	63.59.135.42	137	UDP	Attack
FWIN	3/8/2002	1:24:03 PM	64.208.185.196	4391	63.59.135.42	27374	TCP (flags:S)	Trojan
FWIN	3/8/2002	12:58:41 PM	63.253.214.115	2788	63.59.135.42	27374	TCP (flags:S)	Trojan
FWIN	3/8/2002	12:56:26 PM	205.252.89.19	53748	63.59.135.42	21	TCP (flags:S)	Attack
FWIN	3/8/2002	12:53:04 PM	213.168.122.250	2938	63.59.135.42	27374	TCP (flags:S)	Trojan
FWOUT	3/8/2002	11:21:24 AM	63.59.135.42	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/8/2002	10:09:15 AM	63.34.220.76	1643	63.59.135.146	27374	TCP (flags:S)	Trojan
FWIN	3/8/2002	4:58:47 AM	63.170.184.91	1677	63.59.135.146	80	TCP (flags:S)	Harmless
FWIN	3/8/2002	4:32:05 AM	202.181.213.53	21	63.59.135.146	21	TCP (flags:SF)	Attack
FWIN	3/8/2002	4:26:55 AM	63.170.184.91	4094	63.59.135.146	80	TCP (flags:S)	Harmless
FWIN	3/8/2002	3:16:23 AM	63.217.43.230	2609	63.59.135.146	515	TCP (flags:S)	Scan
FWIN	3/8/2002	3:09:07 AM	63.195.245.108	137	63.59.135.146	137	UDP	Attack
FWIN	3/8/2002	1:12:38 AM	218.17.68.40	0	63.59.135.146	0	ICMP (type:8/subtype:0)	Harmless
FWIN	3/7/2002	8:08:40 PM	64.52.49.99	1090	63.59.135.146	38293	UDP	Unknown
FWIN	3/7/2002	4:37:29 PM	63.151.230.4	4929	63.59.135.146	80	TCP (flags:S)	Harmless
FWIN	3/7/2002	2:05:07 PM	67.192.65.81	2274	63.59.135.146	27374	TCP (flags:S)	Trojan
FWIN	3/7/2002	1:21:12 PM	12.248.109.252	1855	63.59.135.146	27374	TCP (flags:S)	Trojan
FWIN	3/7/2002	1:20:54 PM	62.153.81.82	5636	63.59.135.146	22	TCP (flags:S)	Scan
FWIN	3/7/2002	11:54:42 AM	210.72.110.235	1646	63.59.135.146	80	TCP (flags:S)	Harmless
FWOUT	3/7/2002	10:31:57 AM	63.59.135.146	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/7/2002	5:20:27 AM	216.200.14.231	0	63.59.135.195	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/7/2002	3:28:02 AM	142.165.132.206	1028	63.59.135.195	137	UDP	Attack

FWIN	3/7/2002	2:31:53 AM	203.197.4.98	1025	63.59.135.195	137	UDP	Attack
FWIN	3/7/2002	2:03:59 AM	63.24.123.30	4029	63.59.135.195	80	TCP (flags:S)	Harmless
FWIN	3/6/2002	11:54:10 PM	195.14.141.69	1027	63.59.135.195	137	UDP	Attack
FWIN	3/6/2002	11:09:09 PM	202.110.184.253	4540	63.59.135.195	80	TCP (flags:S)	Harmless
FWIN	3/6/2002	2:21:33 PM	168.215.245.83	2368	63.59.135.195	53	TCP (flags:S)	Attack
FWOUT	3/6/2002	10:30:14 AM	63.59.135.195	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWIN	3/6/2002	10:10:08 AM	64.59.59.91	4790	63.59.135.158	23	TCP (flags:S)	Scan
FWIN	3/6/2002	7:49:23 AM	64.230.91.3	1531	63.59.135.158	21	TCP (flags:S)	Attack
FWIN	3/6/2002	4:40:36 AM	162.33.234.67	3072	63.59.135.158	80	TCP (flags:S)	Harmless
FWIN	3/6/2002	1:58:10 AM	63.216.243.35	2766	63.59.135.158	80	TCP (flags:S)	Harmless
FWIN	3/5/2002	10:56:22 PM	61.129.76.66	4098	63.59.135.158	23	TCP (flags:S)	Scan
FWIN	3/5/2002	10:19:58 PM	62.104.156.12	4415	63.59.135.158	111	TCP (flags:S)	Scan
FWIN	3/5/2002	7:55:14 PM	146.188.144.86	0	63.59.135.158	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/5/2002	7:55:13 PM	146.188.200.73	0	63.59.135.158	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/5/2002	7:52:57 PM	206.132.110.193	0	63.59.135.158	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/5/2002	6:52:01 PM	63.121.98.117	2940	63.59.135.158	80	TCP (flags:S)	Harmless
FWIN	3/5/2002	5:50:15 PM	63.150.156.10	4830	63.59.135.158	80	TCP (flags:S)	Harmless
FWIN	3/5/2002	5:32:18 PM	211.123.199.194	2742	63.59.135.158	111	TCP (flags:S)	Scan
FWIN	3/5/2002	2:41:04 PM	193.115.182.148	3215	63.59.135.158	113	TCP (flags:S)	Harmless
FWIN	3/5/2002	2:22:00 PM	63.76.192.111	137	63.59.135.158	137	UDP	Attack
FWIN	3/5/2002	1:37:12 PM	210.225.227.195	4821	63.59.135.158	515	TCP (flags:S)	Scan
FWIN	3/5/2002	1:35:59 PM	61.152.134.101	4738	63.59.135.158	111	TCP (flags:S)	Scan
FWIN	3/5/2002	12:11:32 PM	64.52.49.99	1090	63.59.135.158	38293	UDP	Unknown
FWOUT	3/5/2002	10:14:57 AM	63.59.135.158	0	206.251.6.192	0	ICMP (type:8/subtype:0)	
FWOUT	3/5/2002	10:08:50 AM	63.59.135.151	0	198.6.1.150	0	ICMP (type:3/subtype:3)	
FWOUT	3/5/2002	10:03:35 AM	63.59.135.151	0	198.6.100.150	0	ICMP (type:3/subtype:3)	
FWOUT	3/5/2002	8:58:01 AM	63.59.135.151	0	198.6.100.150	0	ICMP (type:3/subtype:3)	
FWOUT	3/5/2002	8:01:22 AM	63.59.135.151	0	198.6.1.150	0	ICMP (type:3/subtype:3)	
FWOUT	3/5/2002	7:55:11 AM	63.59.135.151	0	198.6.100.150	0	ICMP (type:3/subtype:3)	
FWIN	3/5/2002	4:47:25 AM	195.14.176.100	137	63.59.135.151	137	UDP	Attack
FWIN	3/5/2002	4:35:01 AM	210.220.16.97	1377	63.59.135.151	111	TCP (flags:S)	Scan

FWOUT	3/5/2002	2:07:46 AM	63.59.135.151	0	198.6.1.150	0	ICMP (type:3/subtype:3)	
FWOUT	3/5/2002	2:07:41 AM	63.59.135.151	0	198.6.100.150	0	ICMP (type:3/subtype:3)	
FWIN	3/5/2002	1:27:21 AM	216.200.14.240	0	63.59.135.151	0	ICMP (type:3/subtype:1)	Harmless
FWIN	3/5/2002	1:25:49 AM	144.134.215.206	1044	63.59.135.151	137	UDP	Attack
FWIN	3/4/2002	3:39:13 PM	12.8.192.232	137	63.59.135.225	137	UDP	Attack
FWIN	3/4/2002	3:16:29 PM	192.168.200.13	137	63.59.135.225	137	UDP	Attack
FWIN	3/4/2002	3:16:29 PM	208.39.142.30	137	63.59.135.225	137	UDP	Attack
FWROUTE	3/4/2002	2:44:50 PM	172.16.0.1	0	172.16.1.34	0	ICMP (type:8/subtype:0)	



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

## Appendix C -- Inadequately Addressed Problems

Based on the analysis undertaken in developing this paper, several shortcomings were uncovered. This section addresses three of these shortcomings and proposes possible solutions.

### C.1 User Warning on Impending Disk Failure

Almost nothing is as heart rending to a consultant out in the field as a disk crash in their laptop, knowing that the scraping sound they hear means, “If it isn’t backed up, it is now gone!” Technology has improved considerably over the past several years and disk crashes that were once seen as totally unpredictable random events are becoming predictable, providing one has the technology installed on the laptop to provide the prediction. The initial efforts in this area resulted in the development of the S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) open standard. The online PC Guide explains,

The fundamental principle behind SMART is that many problems with hard disks don't occur suddenly. They result from a slow degradation of various mechanical or electronic components. SMART evolved from a technology developed by IBM called Predictive Failure Analysis or PFA. PFA divides failures into two categories: those that can be predicted and those that cannot. Predictable failures occur slowly over time, and often provide clues to their gradual failing that can be detected. An example of such a predictable failure is spindle motor bearing burnout: this will often occur over a long time, and can be detected by paying attention to how long the drive takes to spin up or down, by monitoring the temperature of the bearings, or by keeping track of how much current the spindle motor uses.<sup>11</sup>

IBM describes S.M.A.R.T. as,

S.M.A.R.T. is a technology designed to enable a hard drive to predict impending catastrophic failure. S.M.A.R.T. is implemented in hard drive microcode. To use S.M.A.R.T., a system OEM writes software that reads the S.M.A.R.T. status at the ATA or SCSI interface and presents the S.M.A.R.T. status to the end user. In the latest S.M.A.R.T. revision, commands can also perform some self-testing of the hard drive.<sup>12</sup>

On the same page, IBM points out that S.M.A.R.T. is a step in a continuing process. Executive Software, in describing the advanced features of their DiskAlert product state,

<sup>11</sup> The PC Guide, “Self-Monitoring Analysis and Reporting Technology (SMART),” <http://www.pcguides.com/ref/hdd/perf/qual/featuresSMART-c.html>

<sup>12</sup> “IBM Drive Fitness Test,” <http://www.storage.ibm.com/hdd/technolo/dft/dft.htm>

However, each disk manufacture implements SMART to their own specifications. Since these implementations vary from manufacturer to manufacturer, it is difficult to monitor them consistently through one GUI.

DiskAlert does utilize SMART data being sent from SMART enabled disk drives. However DiskAlert goes far beyond SMART by collecting key data from disk drives and using our special algorithms to determine the health of a disk drive. DiskAlert is the most reliable indicator of potential disk failure.<sup>13</sup>

Because of these advances in technology and its availability in off-the-shelf products, inclusion of one of these disk monitoring tools in the standard image would warn the consultant of that most feared disasters, a disk crash, is impending. With that warning, the consultant might advance a scheduled full backup, just in case. Since this problem affects desktop systems and servers as well as laptops, standardizing on one tool across the company is prudent.

## C.2 Encrypted Disks

As JSI points out in their earlier referenced registry hack description, “Lost your Administrator password and need the ultimate hack?” once someone has their hands on a laptop, getting past all the passwords is a relatively trivial matter. Encrypting the NTFS partitions would be a useful step to consider. The obvious incompatibility of NTFS disk encryption and NTFS disk compression can be overcome by larger disks and tape devices for backup.

## C.3 Advertisement/Popup Filter

I mentioned in Section 1.5.7 the effect popup ads, particularly the X-rated ones, can have on clients and believe strongly that the basic system image for laptops, particularly ones that accompany consultants to client sites, must include a utility to suppress advertisements and popups. A popup filter has been added to ZoneAlarm Pro, but my experience indicates this portion of the program is fairly immature and does not permit “tuning” to prevent it from suppressing useful functionality. Other tools, such as AdSubtract<sup>14</sup>, provide a much finer, site-specific level of control.

Since the company now subscribes to a service that provides filters web pages based on content, issuing warnings to users who may have been inadvertently directed to the page, extending the availability of this tool throughout the company would actually provide the Company an additional benefit by freeing up some currently utilized bandwidth.

---

<sup>13</sup> “DiskAlert FAQs,” <http://www.diskalert.com/diskalert/faqs/faqs.asp>

<sup>14</sup> “AdSubtract.com – We Subtract the Ads!” <http://www.adsubtract.com/>

## Bibliography

"2002 CSI/FBI Computer Crime and Security Survey," Volume VIII, Number 1, Spring 2002, Computer Security Institute

"A quick guide to email security," Paul Slavic, [http://www.zzee.com/email\\_security](http://www.zzee.com/email_security)

"Accounts with No Passwords or Weak Passwords," **The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts' Consensus**, Version 2.503 April 8, 2002, SANS Institute.

"AdSubtract.com - We Subtract the Ads!" <http://www.adsubtract.com/>

"Anti-Piracy FAQ," Software & Information Industry Association, <http://www.spa.org/piracy/faq/default.asp>

"Anti-Trojan Online Check," Anti-Trojan, <http://www.anti-trojan.net/at.asp?l=en&t=onlinecheck>

"Anti-Virus test file," eicar online, [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

"Best Practices for Applying Service Packs," **Hotfixes and Security Patches**, Microsoft Corporation, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secure.asp>

"Browser Spy," gmal.dk, <http://www.gemal.dk/browserspy/>

"Checklist: Assess Your Risk," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/assess.asp>

"Checklist: Check Your Security Settings," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/settings.asp>

"Checklist: Conduct routine security maintenance," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/maintenance.asp>

"Checklist: Create Strong Passwords," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/password.asp>

"Checklist: Install a Firewall," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/firewall.asp>

"Checklist: Keep Software Up-To-Date," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/update.asp>

"Checklist: Use Anti-Virus Software," 7 Steps to Personal Computing Security, Microsoft Corporation, <http://www.microsoft.com/security/articles/antivirus.asp>

"Description of the Windows Critical Update Notification Utility (Q224420)," Microsoft Corporation, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q224420>

"DiskAlert FAQs," Executive Software, <http://www.diskalert.com/diskalert/faqs/faqs.asp>

"Electronic Data Security Awareness," Phillip A. Grove, SANS Information Security Reading Room, SANS, November 29, 2000, [http://rr.sans.org/securitybasics/electronic\\_datasec.php](http://rr.sans.org/securitybasics/electronic_datasec.php)

"FAQ about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool (Q305385)," Microsoft Corporation, <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q305385>

"Five laptop security musts for users," Mike Walton, **TechRepublic**, 06 May 2002, <http://www.zdnet.com.au/newstech/security/story/0,2000024985,20265023,00.htm>

"G3 - Non-existent or Incomplete Backups," **The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts' Consensus**, Version 2.503 April 8, 2002, SANS Institute;

"Guarding Your Laptop at the Airport," Sarah Cusick, Business Travel column on About.com, <http://businesstravel.about.com/library/weekly/aa080898.htm>

"Hfnetchk.exe Returns NOTE Messages for Installed Patches (Q306460)," Microsoft Corporation, <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306460>

"HotFix & Security Bulletin Service," Microsoft Corporation, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp>

"How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261)", Microsoft Product Support Services, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q246261>

"IBM Drive Fitness Test," IBM Corporation, <http://www.storage.ibm.com/hdd/technolo/dft/dft.htm>

"ID and Password Recovery," Notes Net,  
<http://www.notes.net/today.nsf/f01245ebfc115aaf8525661a006b86b9/2bc078be1aa6095285256af70059dd3a?OpenDocument>

"Installing and Securing an Existing Windows 2000 System," Microsoft Corporation,  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/w2kexist.asp>

"IT Baseline Protection Manual, Chapter 5.3 Laptop PC," Bundesamt für Sicherheit in der Informationstechnik (BSI), <http://www.bsi.bund.de/gshb/english/b/53.htm>

"Laptop Computer Security," Richard Childers, **SANS Institute Reading Room**, October 30, 2000, <http://rr.sans.org/homeoffice/laptop.php>

"Laptop Computer Security: White Paper," **Caveo Technology**,  
<http://www.caveo.com/images/anti-theftwhitepaper.pdf>

"Laptop Security: Be Deliberate," Mark Joseph Edwards, **Security Administrator**, September 21, 2000, <http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=15653>

"Laptop Security," Honors Laptop Program, Temple University,  
<http://www.sbm.temple.edu/laptop/security.html>

"Laptop Security," U.S. Army Material Command,  
<http://eaglenet.robins.af.mil/cio/laptop.htm>

"Laptop Security: Past, Present," Andrew Mueller, **SANS Information Security Reading Room**, July 10, 2001, [http://rr.sans.org/travel/laptop\\_sec.php](http://rr.sans.org/travel/laptop_sec.php)

"Laptop Security Guidelines," LabMice.Net,  
<http://www.labmice.net/articles/laptopsecurity.htm>;

"Laptop security needs to be a priority, officials say," Joshua Dean, Daily Briefing, **GovExec.com**, August 8, 2001, <http://www.govexec.com/dailyfed/0801/080801j1.htm>

"Laptop Security Tips," Garry McGonigal, **CancerLynx**,  
<http://www.cancerlynx.com/laptoptips.html>

"Lessons in laptop security," Jeff Zbar, Networker, Network World, 03/26/01,  
<http://www.nwfusion.com/net.worker/columnists/2001/0326zbar.html>

"Locking Down the Laptop," Paul Korzeniowski, Information Security, February 2001,  
[http://www.infosecuritymag.com/articles/february01/features\\_laptop\\_security.shtml](http://www.infosecuritymag.com/articles/february01/features_laptop_security.shtml)

"Look Out for Your Laptop: Information Security and Laptop Theft Prevention" a training video, **Commonwealth Films**, <http://www.commonwealthfilms.com/3030.htm>

"Lost your Administrator password and need the ultimate hack?" JSI, INC., <http://www.jsiinc.com/subb/tip0500/rh0554.htm>

"Lotus Notes Frequently Asked Questions," Division of Information Technology, Stony Brook University, <http://clientsupport.stonybrook.edu/notes.shtml>

"Microsoft Baseline Security Analyzer," Microsoft Corporation, <http://www.microsoft.com/security/tools/Tools/MBSAWP.asp>

"Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available (Q303215)," Microsoft Corporation, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215>

"Microsoft Office Update," Microsoft Corporation, <http://office.microsoft.com/productupdates>

"Microsoft Windows Update, Microsoft Corporation, <http://windowsupdate.microsoft.com/>

"Online Security Services," Bruce Stewart, **ZDNet Reviews & Solutions**, December 1, 2000, <http://www.zdnet.com/products/stories/reviews/0,4161,2422273-1,00.html>

"Port Scan," IPchains.net, [http://www.ipchains.net/Port\\_Scan/port\\_scan.php](http://www.ipchains.net/Port_Scan/port_scan.php)

"Security in Windows 2000," Gene Schultz, SANS Course Book, SANS, October 15, 2000.

"Security memo to Bill Gates: Security issues in Microsoft desktop products," Richard M. Smith, **Computerbytesman**, January 17, 2002, <http://computerbytesman.com/security/bill1.htm>

"Security Statistics – Laptop Theft," **Notebook Security**, Kensington Technology, [http://www.micosaver.com/tips/tip\\_1028.html](http://www.micosaver.com/tips/tip_1028.html)

"Security tool leaves holes," **eWeek**, Volume 19, Number 16, April 22, 2002.

"Self-Monitoring Analysis and Reporting Technology (SMART)," **The PC Guide**, <http://www.pcguide.com/ref/hdd/perf/qual/featuresSMART-c.html>

“Seven Steps to Personal Computing Security,” Microsoft Corporation,  
[http://www.microsoft.com/security/articles/steps\\_default.asp](http://www.microsoft.com/security/articles/steps_default.asp)

“ShieldsUP!,” Gibson Research Corporation, <http://grc.com/default.htm>,

“Theft of data tops security woes,” Reuters, April 7, 2002, <http://news.com.com/2100-1001-877427.html>

“Theft of Qualcomm chairman's laptop provides security lessons for users,” Jaikumar Vijayan, **ComputerWorld**, September 19, 2000,  
<http://www.computerworld.com/securitytopics/security/story/0,10801,50710,00.html>

“TP General - How to remove/add/change a power on password,” IBM ThinkPad Support, IBM Corporation. <http://www.pc.ibm.com/qtechinfo/YAST-3JZNDP.html>

"Use QChain.exe to Install Multiple Hotfixes with Only One Reboot (Q296861)," Microsoft Corporation, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861>

“Virus Check.” Zimbabwe OnLine Services, <http://www.virustest.co.zw/>

"Windows 2000 Professional Configuration," Windows 2000 Professional Baseline Security Checklist, Microsoft Corporation,  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklis/t/w2kprocl.asp>

"ZZEE Email Not HTML: gracefully handles HTML based email,"  
[http://www.zzee.com/enh/-zzee\\_link\\_3\\_1014864770](http://www.zzee.com/enh/-zzee_link_3_1014864770)

© SANS Institute 2000-2002. All rights reserved.