



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>

SANS GSNA CERTIFICATION
GSNA (AUDITING NETWORKS, PERIMETERS AND SYSTEMS) v 3.0

AUDITING THE SECURITY POSTURE OF A SOHO MACHINE
AN AUDITOR'S PERSPECTIVE – OPTION 1

Submitted by: Nicole Christopher
Date: March 16, 2004

Abstract

With screaming headlines about the latest viruses and hacker exploits, security on the Internet is an ever-growing concern for businesses both large and small. However, while the larger counterparts have strengthened their security postures to mitigate risks, SOHOs (Small Office Home Office) due to budget constraints are still operating with security holes that make them more attractive targets for attackers on the prowl.

The focus of this audit is a typical home-based system that operates both as the business and personal PC. The key components of the system to be looked at are the O/S, the applications and the dedicated cable modem connection. The owner also doubles as the administrator and has limited access to and knowledge of the latest IT Security tools in order to properly assess the security of the system. Therefore, my task as the auditor is to first determine if adequate protection is in place and second provide appropriate recommendations for risk mitigation.

This paper should find an useful audience in the growing number of telecommuters, home business owners and generally anyone conducting e-commerce, personal banking, research or other electronic transmittal and storage of sensitive data. More importantly, it will provide a comprehensive audit reference that can be used by other auditors faced with a similar task of baselining a SOHO system.

© SANS Institute 2004, Author retains full rights.

Table of Contents

Part 1 - Research in Audit, Measurement Practice and Controls

- 1.1 - Identify the System to be audited..... Pg 4
- 1.2 - Evaluate the most significant risk to the system..... Pg 4
- 1.3 - What is the current state of practice?..... Pg 14

Part 2 – Create an Audit Checklist

- 2.1 – Operating System Audit Checklist..... Pg 19
 - 2.1.1 – Checking for Default Installations..... Pg 22
 - 2.1.2 – Checking for Unpatched Systems..... Pg 22
 - 2.1.3 – Checking for Outdated Virus Definitions..... Pg 22
- 2.2 – Network/Cable Modem Audit Checklist..... Pg 23
 - 2.2.1 – Checking for Perimeter Protection..... Pg 23
- 2.3 – Application Audit Checklist..... Pg 26
 - 2.3.1 – Checking for Faulty Installations..... Pg 26
 - 2.3.2 – Checking for Unknown Downloads..... Pg 26
 - 2.3.3 - Checking for Outdated Virus Protection..... Pg 27
 - 2.3.4 – Checking for Weak Protection of Sensitive Data..... Pg 27
- 2.4 – Operational Audit Checklist..... Pg 28
 - 2.4.1 – Checking for Data Retention Protection..... Pg 28
- 2.5 – Physical/Environmental Audit Checklist..... Pg 29
 - 2.5.1 – Checking for Sufficient Fire Detection/Suppression..... Pg 29

Part 3 – Conduct the Audit – Testing, Evidence and Findings

- 3.1 – Operating System Audit Results..... Pg 30
 - 3.1.1 – Checking for Default Installations..... Pg 30
 - 3.1.2 – Checking for Unpatched Systems..... Pg 31
 - 3.1.3 – Checking for Outdated Virus Definitions..... Pg 32
- 3.2 – Network/Cable Modem Audit Results..... Pg 32
 - 3.2.1 – Checking for Perimeter Protection..... Pg 32
- 3.3 – Application Audit Results..... Pg 32
 - 3.3.1 – Checking for Faulty Installations..... Pg 32
 - 3.3.2 – Checking for Unknown Downloads..... Pg 32
 - 3.3.3 - Checking for Outdated Virus Protection..... Pg 33
 - 3.3.4 – Checking for Weak Protection of Sensitive Data..... Pg 33
- 3.4 – Operational Audit Results..... Pg 33
 - 3.4.1 – Checking for Data Retention Protection..... Pg 33
- 3.5 – Physical/Environmental Audit Results..... Pg 33
 - 3.5.1 – Checking for Sufficient Fire Detection/Suppression..... Pg 33

Part 4 –Audit Report

- 4.1 – Executive Summary..... Pg 33
- 4.2 – Audit Findings..... Pg 34
- 4.3 – Audit Recommendations..... Pg 35

Part 1 - Research in Audit, Measurement Practice and Controls

1.1 - Identify the system to be audited

I am auditing a Small Office Home Office (SOHO) system. This system comprises of a Dell Dimension 8250; running Microsoft Windows XP Home Edition v2002; with a Pentium 4 (2.66 GHz) processor. The client is the single user and indicates that there are no other accounts established. The primary role of the system is for a home-based financial consulting/tax preparation business and it has primarily the Microsoft Office suite, tax preparation and finance software. The client also indicates that there is none of the popular peer-to-peer file sharing and instant messaging software installed. The system also supplements the client's personal use for online banking and e-mail. The system is connected to the Internet via a Toshiba PCX2500 cable modem. It has a local connection to a HP Office Jet T45xi All-In-One which handles all of its copying, faxing, scanning and printing needs. This system needs to be securely configured as it provides daily access for the critical business services.

1.2 - Evaluate the most significant risk to the system

In determining *risk* to a system, one has to identify what poses a *threat* to the triad - Confidentiality, Integrity and Availability (C.I.A.). Once threats have been identified, it is key to estimate their likelihood and whether exploitable by a *vulnerability* of the system. All risks are not addressable and cannot be totally eliminated. Therefore it is imperative that the security controls/safeguards are focused against threats that pose the greatest danger.

The Microsoft Windows platform is infamously known as being full of security flaws, yet it remains the most popularly deployed O/S on desktops that require low-end processing capabilities. To counter this, the Microsoft Windows XP platform was introduced to address major Microsoft Windows vulnerabilities. However, the XP platform (even though more secure than its Microsoft predecessors) has still been the target of attacks due to unaddressed or newly discovered vulnerabilities.

The biggest vulnerability to be addressed is running Microsoft Windows XP in its default configuration with unprotected accounts, unnecessary services and open ports. Once the O/S has been hardened, then its secure configuration must be maintained via subscriptions, alerts, and automatic updates. Another vulnerability, that seems to be equally as serious, is the 'always-on' dedicated cable modem connection that has no perimeter defenses other than Microsoft Windows XP's built-in firewall mechanism. Lastly, is the plethora of application viruses and worms usually written against Microsoft software.

While there are many assets important to sustaining the livelihood of this SOHO, not all can be equally protected due to budgetary constraints. So while safeguards will be put in place as widely possible, special attention must be

given to those assets deemed most critical to the business. Since this is a financial consulting/tax preparation business, the major information asset in providing financial services and data, appears to be the desktop system and not the other peripherals.

However, in determining the criticality of an asset, one has to first determine its value to the business. After a thorough research of its business model, each asset was valued based on revenue streams; cost to acquire/recover and competitive worth. The values for this Business Impact Analysis (BIA) were calculated as follows:

Desktop (Data & Services)

Asset Value (AV) = \$273 (Daily revenue) -> \$100,000 (Yearly revenue)
\$3000 (Cost)
\$2000 (Cost of database of client leads)

Exposure Factor (EF) = Percentage of asset loss if the computer services were unavailable for an 8hr business day; -\$69 (Daily revenue) -> -\$25,000 (Yearly revenue); 75%

Direct Impact = Immediate financial impact of asset loss; $.75 \times \$100,000 \rightarrow -\$75,000$

Indirect Impact = Indirect business impact of counteracting asset loss (Dollars spent on new system; alternate transaction processing – paper/phone; rebuilding clientele); Estimated at - \$10,000

Cable Modem

Asset Value (AV) = \$100 (Cost for replacement/installation)

Exposure Factor (EF) = Percentage of asset loss if the internet services were unavailable for an 8hr business day would be none to the cable modem. However, such unavailability affects access to data and services. This is limited due to available alternate communication (phone/fax) for research data. It was estimated to affect the daily revenue stream by -\$2 -> -\$728 (Yearly); .00728%

Direct Impact = Immediate financial impact of asset loss; $.00728 \times \$100,000 \rightarrow -\728

Indirect Impact = Indirect business impact of counteracting asset loss (Dollars spent on new system; reinstallation costs); Estimated at -\$100

Phone

Asset Value (AV) = \$40 (Cost for replacement)

Exposure Factor (EF) = Percentage of asset loss if the phone services were unavailable for an 8hr business day would be none as a backup cellular phone is available; N/A

Direct Impact = N/A

Indirect Impact = Indirect business impact of counteracting asset loss (Dollars spent on new system); Estimated at -\$40

Copier/Facsimile/Printer/Scanner

Asset Value (AV) = \$350 (Cost for replacement)

Exposure Factor (EF) = Percentage of asset loss if the office support services were unavailable for an 8hr business day would be negligible in terms of continuity of providing data and services. The alternatives are many including e-faxing, e-mailing and outside services. It was estimated to affect the daily revenue stream by -\$1 -> -\$364 (Yearly); .00364%

Direct Impact = Immediate financial impact of asset loss; $.00364 \times \$100,000 \rightarrow -\364

Indirect Impact = Indirect business impact of counteracting asset loss (Dollars spent on new system); Estimated at -\$350

My research led to some computations that were used to quantify each of the variables in this preliminary assessment. These were taken from **Microsoft TechNet: "Understanding the Security Risk Management Discipline". Security Policy, Assessment, and Vulnerability Analysis**

URL: <http://www.microsoft.com/technet/security/topics/assess/default.mspx>

- ❖ Assign a threat probability (TP) (0% lowest – 100% highest). The threat probability is the probability of a possible threat agent entering your environment.
- ❖ Assign a criticality factor (CF) (1 lowest – 10 highest). The criticality factor is the level of potential exploit of the threat to an asset.
- ❖ Rank the effort (E) (1 lowest – 10 highest). The effort represents the skills required for an attacker to take advantage of the exploit.
- ❖ Determine the risk factor (RF). This is the criticality factor divided by effort.
- ❖ Determine the threat frequency level using the equation (TP x RF).
- ❖ Rank the vulnerability factor (VF) (1 lowest – 10 highest). Decide how big of a risk the vulnerability will be to an asset.
- ❖ Determine the asset priority (AP) (1 lowest – 10 highest).
- ❖ Determine the impact factor (IF) using the equation (VF x AP).

Collectively, the following tables were used to evaluate the most significant risk. **Table 1.2.1** enumerates a list of possible threats and damage capacity based on **Impact Factor (IF)** values; the information assets most critical to the business and at risk due to these threats are evaluated in **Table 1.2.2**; the desktop system is assigned an **Asset Priority (AP)** of **10** - most critical - upon taking its **Asset Value, Exposure Factor and Direct/Indirect Impact** into consideration; **Tables 1.2.3.1- 1.2.3.5** explore each vulnerability that could evolve into a realized threat and its potential impact.

Table 1.2.1

Threats

Operating System	Damage Capacity (Based on IF values)
Service Disruptions Attacks	High
Windows Improper Authentication	Low
Malware	High
Cable Modem/Network	Damage Capacity (Based on IF values)
Theft of Service	Low
Perimeter Penetration	High
Applications	Damage Capacity (Based on IF values)
Service Disruption Attacks	High
Improper Information Disclosure & Alteration	Medium
Malware	High
Operational	Damage Capacity (Based on IF values)
Logon Abuse	Low
Data Loss	Medium
Multiple Users	Low
Physical /Environmental	Damage Capacity (Based on IF values)
Physical theft/damage	Low
Interruption in computer services	Low

Electrical, Fire & HVAC insufficiencies	Medium
--	---------------

Table 1.2.2

Information Asset Valuation and Prioritization

Desktop			System		
Asset Description	Asset Value	Exposure Factor	Direct Impact	Indirect Impact	Asset Priority
Computer Financial Services <ul style="list-style-type: none"> Tax Preparation Securities E-Trading Computer Data <ul style="list-style-type: none"> Client Data Research Data 	\$100K	.75	\$75K	\$10K	10
Peripherals					
Asset Description	Asset Value	Exposure Factor	Direct Impact	Indirect Impact	Asset Priority
Phone <ul style="list-style-type: none"> Communication 	\$40	N/A	N/A	\$40	1
Cable Modem <ul style="list-style-type: none"> Network Connection 	\$100	.00728	\$728	\$100	3
Printer/Fax/Copier <ul style="list-style-type: none"> Office support 	\$350	.00364	\$364	\$350	2

Major Vulnerabilities & Potential Impacts

Table 1.2.3.1

Operating System

Threat	Vulnerability	Impact/Outcome	TP (Threat Probability)	CF (Criticality Factor)	E (Effort)	RF (Risk Factor)	TFL (Threat Frequency Level)	VF (Vulnerability Factor)	IF (Impact Factor)
Service Disruption Attacks (DoS)	Default Installations - No Administrator Pwd - Unused open ports - Unneeded services	- could allow remote access w/ admin privileges - potential for service disruption	8	10	2	5	40	9	90
	TCP Implementation Weakness - Buffer Space exploits - Sequence number guessing	- SYN attack can crash system - Session hijacking attack can allow takeover of system	5	10	8	1.25	6.25	4	40
Windows Improper Authentication	Password Weaknesses - Accounts w/weak or no pws - Legacy LM hashes in SAM - Default LAN Manager enabled - Non-existent pwd policies	-Easier for attacker to gain access -Easier for attacker to obtain pws -Easier for attacker to obtain pws -No pwd enforcement	3	8	4	2	6	2	20

Malware (Trojans & Viruses)	Unpatched Systems -Default O/S with no security patches File and Printer Sharing service - Enabling service	-Leaves system open to a range of known, successful attacks	9	10	2	5	45	9	90
	Outdated Virus Definitions - Not subscribing to an anti-virus service	-Leaves system unprotected against latest Malware & attackers can exploit holes via backdoors, DoS.	9	10	2	5	45	9	90

Table 1.2.3.2

Network/Cable Modem

Threat	Vulnerability	Impact/Outcome	TP (Threat Probability)	CF (Criticality Factor)	E (Effort)	RF (Risk Factor)	TFL (Threat Frequency Level)	VF (Vulnerability Factor)	IF (Impact Factor)
Perimeter Penetration	Always 'on' connection - Advertises static IP address - exploit ICQ - not DOCSIS compliant - Shared Media	- Easier to find in a scan of a 24/7 time frame - Eavesdropping	3	8	7	1.14	3.4	3	9
	Local Resource Sharing Service - May be enabled	- Allows attacker access	8	10	2	5	40	9	27
	No Defense-In-Depth mechanisms - Absence of hardware router/firewall (Only Microsoft ICF)	- Attackers can slip by less sophisticated software firewalls that don't track protocols in a table & filters dynamically - Since IFC is limited to filtering only on incoming ports, trojans & spyware can still use outgoing ports - External firewalls add more layers of protection by hiding static IP addresses via NAT	8	10	4	2.5	20	9	27
Theft of Service	Cable Providers not fully enabling security features -	-Attackers can steal legitimate subscribers' paid	5	9	9	1	5	3	9

		services with counterfeit configuration files; cloned IP & MAC addresses							
--	--	--	--	--	--	--	--	--	--

Table 1.2.3.3

Applications

Threat	Vulnerability	Impact/Outcome	TP (Threat Probability)	CF (Criticality Factor)	E (Effort)	RF (Risk Factor)	TFL (Threat Frequency Level)	VF (Vulnerability Factor)	IF (Impact Factor)
Service Disruption Attacks (DoS)	Faulty Installations - Out-of-the-box installations - Unknown source installations	-Leaves system open to a range of known attacks	5	10	2	5	25	7	70
Malware (Trojans & Viruses)	Unknown downloads - Email attachments - Open application ports - Unnecessary application services	-Leaves system open to a range of known attacks	9	10	2	5	45	9	90
	Outdated Virus Definitions - Not subscribing to an anti-virus service	-Leaves system unprotected against latest Malware & attackers can exploit holes via backdoors, DoS.	9	10	2	5	45	9	90
Improper Information Disclosure and Alteration	Weak protection for sensitive data - lack of encryption - caching	- Could allow attacker to intercept data in transit or stored on servers	5	10	2	5	35	7	70
	Web application holes SERVER - CGI scripts - SQL injections - XXScripting - Hidden forms - Java, JavaScript, ActiveX BROWSER - Executable attachments - Non-use of SSL or TLS for secure data transmission - Non-use of digital certificates, signatures to verify message, sender/receiver - Use of non-secure HTTP instead of secure HTTPS for	-Leaves server open to these specific web application attacks - Allows dangerous files to execute - Attacker can intercept data - Attacker can spoof msgg/sender/receiver - Attacker can change contents of web page	3	10	8	1.25	3.75	3	30

	protection of web page contents - Non-restriction of cookies to enhance privacy - Enabling ActiveX, JavaScript or VBScript -Caching - No lock-out time periods	- Cookies can track your information for attacker - Allows embedded malicious scripts - Saves critical info for attacker - Allows attacker to gain access							
--	--	--	--	--	--	--	--	--	--

Table 1.2.3.4

Operational

Threat	Vulnerability	Impact/Outcome	TP (Threat Probability)	CF (Criticality Factor)	E (Effort)	RF (Risk Factor)	TFL (Threat Frequency Level)	VF (Vulnerability Factor)	IF (Impact Factor)
Logon-on Abuse	- Multiple User Accounts - Unknown source installations	- Falsified data input/tampering	1	10	5	2	2	1	10
Data Loss	- Poor storage of backups - No backup procedures	-Delayed processing - Lost data	5	9	2	4.5	22.5	5	50

Table 1.2.3.5

Physical/Environmental

Threat	Vulnerability	Impact/Outcome	TP (Threat Probability)	CF (Criticality Factor)	E (Effort)	RF (Risk Factor)	TFL (Threat Frequency Level)	VF (Vulnerability Factor)	IF (Impact Factor)
Physical theft/damage	- Unlocked equipment	- Theft of Desktop System	1	10	9	1.1	1.1	1	10
Electrical, Fire & HVAC insufficiencies	Humidity - too high - too low	-Electroplating; Parts corrosion - Static electricity damage	2	6	3	2	4	2	20
	Power fluctuations - Absence of UPS; Surge protectors		2	5	3	1.67	3.34	2	20
	Insufficient Fire Detection/Suppression - Absence of fire extinguisher/alarms	- Equipment Destruction	3	10	2	5	15	5	50

After this preliminary review of the SOHO, it was noted that the threats which presented the greatest risks were service disruption attacks, malware, possible perimeter penetration and physical security insufficiencies. The other areas of concern were also taken into consideration, but their unlikely occurrence or low impact may not warrant extra resources (See Tables 1.2.3.1 – 1.2.3.5).

Here is a recap of each table:

Table 1.2.3.1 shows how the operating system can be threatened by Service Disruption Attacks, Windows Improper Authentication and Malware. With Service Disruption Attacks, default installations seem to be the most likely enabler than weak TCP implementations (although **Criticality Factor = 10** for both). What stands out is the ease of effort in carrying out an attack due to leaving an operating system in its default configurations (**E = 2**) compared to having the knowledge to carry out buffer space and sequence number exploits.

The latter (having an **E = 8**) is not only harder for an attacker to implement, but an updated operating system is very likely to have fixed known TCP issues. An out-of-the box platform running on systems is much more common and because of this prevalence – more dangerous. With little effort required, in considerably no time a *script kiddie* can unleash his/her freebie weapons against published issues of certain services/ports on the platform.

For example, by default, the Windows operating system enables risky services such as resource sharing (File and Printing Sharing Service); and remote access services (RPCs, telnet, ftp, SNMP). These are key ways that an attacker who is not physically at your system can still virtually access and control it.

Windows Improper Authentication has followed each successor of Microsoft Windows due to the retention of weak legacy LM hashes for compatibility with newer versions. Additional concerns are the possible open holes of multiple accounts with improper authentication and privileges due to non-existent or weak passwords. This issue has a **CF** of **8**, coupled with an **EF** of **4**.

This is usually a high concern for administrators. However, since this is a single user system, this issue is easily controlled with straightforward checks against the single password versus management of multiple passwords. Therefore, the **RF** was assigned a value of **2** and treated as a minor risk. Malware is by far the biggest threat (**TP=9**) to both patched and unpatched operating systems. However, having an unpatched system compounds the problem by making it even easier for attackers to compromise the system (**E=2**).

For example, backdoor access can give attacker full system control. Some well-known XP trojans which exploit this are the *\$decode()* and *mIRC* (found in Microsoft XP 6.x versions prior to 6.03). Trojans allow remote code execution and DoS attacks w/out being detected. Viruses like *Nachi* & *Blaster* worms particularly exploit the remote procedure call (RPC) vulnerability which attackers can also use exploit for remote code execution.

An equal co-conspirator in enabling malware is having Outdated Virus Definitions. Attacks are on-going and new malware is a daily threat. Therefore,

by not subscribing to an anti-virus service, one leaves the system unprotected against the latest malware which is a very precarious position to be in.

Table 1.2.3.2 examines the possible insecurities of the Network/Cable Modem. A huge area of concern is the lack of defense-in-depth of the network topology. Although, there is no internal network (no other PC, printer, facsimile, dial-up modem attached by a router or hub), the cable modem provided the network connection to the outside world via the ISP. Therefore, this provides the single access point for the hacker into the desktop which reduces **E** to a value of **4**. The client indicated in the preliminary interview that that he would like to get definitive answers regarding the safety of cable modem as he has been reading conflicting reports.

One view is that its 'always-on' connection advertises a static IP address. This supposedly presents a couple of vulnerabilities – (i) a longer time frame for the attacker to leverage attack tools; (ii) an unchanging identification of your machine to the world. However, research into the properties of the cable modem has shown that IP broadcasts are not propagated throughout the network (a shared media Ethernet property).

Therefore, without this broadcasting capability, the rest of the nodes would not be able to see your node in order to 'sniff' your traffic. This reduces the **TP** to a value of **3** because the skill level necessary to launch an eavesdropping exploit on this type of media would require more sophisticated packet capturing tools than readily available sniffer tools (an **E** of **7**).

Cable modems also offer access to local shared resources (much like the Windows operating systems). And, they also may be guilty of having other default and unnecessary services running. Again, these present possibilities of remote attacks into the system. With an **E** of **2**, these known holes can be easily exploited and so must be addressed as the **TP** is relatively with a value of **8**.

The key is to use a modem that is DOCSIS compliant and possibly has a built-in firewall - which is an easy check. DOCSIS (Data Over Cable Service Interface Specification) includes standards that allow x.509 certifications to be issued to the cable modems; Baseline Privacy Specifications that ensure privacy in end to end communications; and an additional layer of security with DES/3DES encryption (AES upgrade likely) from the modem to the modem termination system; and RSA public key encryption.

Cable IP networks are often mistakenly believed to be insecure ...However, the cable IP network can be an extremely secure access medium – at least as secure as other common access media. The DOCSIS specifications, along with advanced features available on some CMTS platforms, enable cable operators to effectively combat security risks through simple means. DOCSIS shared secrets, BPI+, and other cable IP network features can mitigate all but the most aggressive attacks. When deployed, DOCSIS security features can help create a cable IP access network as secure as any circuit-switched point-to-point access network.

McKelvey, Joel T. Cisco Systems, Inc., USA. "Combating security risks on the cable IP network."

URL: <http://www.broadcastpapers.com/broadband/IBCCiscoSecurityCableIP01.htm>

This brings us back to the examination of whether a defense-in-depth architecture needs to be built. The idea here is to 'buy time' or make it harder for the attacker by increasing the level of difficulty for the attack in at least one dimension – time. Since the Windows XP platform does have a firewall for this additional security layer, the audit needs to focus on its effectiveness in denying access appropriately so that a decision can be made on whether or not a hardware version may provide protection.

As the perimeter (OSI Layer 3) becomes more secure, application attacks (OSI Layer 7) are now more prevalent. Therefore the possible risks within the few applications being used could not be overlooked. However, special attention was given only to the web browser and not the list of the very few commercial applications installed.

It was felt that resources were better directed at the web browser, but still as a backup measure of security (check for the latest anti-malware security controls against the installed tax software; spreadsheet and word processing applications). This can be automated and checks for unknown source code and hidden executable code. With a subscription to anti-virus services, these controls are very likely to be in place and can be easily checked.

Web application security cannot be overlooked as these types of applications are the target of many attacks. Although the business does conduct e-commerce transactions, it does not host its own web services. This eliminates the first area of concern – a web server – against which the typical attacks are launched such as CGI scripts, URL attacks, Parameter/Content/Input Tampering. Our concern can then be focused on the web browser being utilized to ensure that the sensitive web traffic does not get compromised.

The web browser in use by default is Internet Explorer version 6.0 and it has its own list of issues. Since this client connects to a remote host to conduct financial transactions and review sensitive data for his customers, lack of encryption in the browser can seriously compromise his business. Another feature of the browser that can cause security breaches is its default caching mode – which speeds up memory - but also saves critical information for the attacker to later access. The danger here is the ease of an attack on a browser's data without weak data protection controls (**E=2; TP=7**).

The effort required to carry out most serious web application exploits does require some knowledge of CGI Java & ActiveX scripting, SQL injections; Cross-site scripting; using Hidden forms to manipulate the back-end servers that house the data. Hopefully, these are properly addressed at the host server's site and so these vulnerabilities are not directly applicable to this environment - even though highly critical (**CF = 10; RF = 1.25**). On our end, we still need to harden the web browser to make sure that the data being manipulated is as secure as possible (against known Microsoft IE exploits) whether stored or in transit.

Often overlooked are the less technical areas that are still quite as important to the livelihood of the business. Logon abuse and inappropriate use

are eliminated as concerns because the client is the sole system user. As we know this can still be circumvented by password and account mismanagement, however, these checks were incorporated into earlier technical controls.

Similarly, the threats of physical theft/damage and electrical/HVAC insufficiencies were found to be fairly unlikely (as evident by low **RF** values). On the other hand, significant vulnerabilities existed for possible threats of service interruption due to data loss or inadequate fire protection. So, the necessary checks were put into place to counter these.

The components at risk were critical to the successful delivery of the SOHO's business services. It is clear to see just how at risk when utilizing the scores from the risk analysis as it quantifies each variable. One notices high scores for **Impact Factor (IF)** against the operating system, cable modem, applications and to a lesser extent operational/physical/environmental issues. Equally as important is the **Effort (E)** required for successful attacks, because the higher (or harder) it is, the lower the **Risk Factor (RF)**, regardless of the criticality or **Critical Factor (CF)**.

In other words, although it would be devastating if an attacker were to physically steal the desktop system, but because it would require surpassing several, well-appointed physical access controls then the risk is deemed fairly low. This inverse mapping of **Effort (E)** to **Risk Factor (RF)** was helpful for me as an auditor in deciding the most significant risk and where to direct my resources.

Based on three combined critical values (**TP** > 8; **CF** • 10; **IF** > 90), service disruption attacks and malware unleashed on the operating system and applications appear to present the greatest risks. The other noted threats (even with lower critical values) are pretty serious threats and appropriate resources should be levied accordingly. In order to properly apply controls and safeguards, it is absolutely necessary for thorough research of best practices being utilized industry-wide.

1.3 - What is the current state of practice?

Currently the security posture of most SOHOs in comparison to larger organizations - is not where it should be. Most small shops operate under insecure configurations due to limited resources and knowledge. "...Small businesses can't seem to justify the amount of money that is needed to build a secure infrastructure for their business... One must protect that website, stay current on exploits, monitor traffic to and from their network and stay current with technologies. That is a lot to ask a small business owner." Ray, Cody. "Maximum Security in Small Business". 16 May, 2001.

URL: http://www.group1ifw.com/whitepapers/maximum_security.htm

As a result, most SOHOs run on the Windows platform instead of the more resource intensive UNIX platform. Yet, with Windows' wide deployment also comes more security issues - both known exploits and unknown vulnerabilities. Microsoft XP has addressed security threats by providing a built-in personal firewall (Internet Connection Firewall (ICF)). A hardware or software firewall is one type of control that can be put in place to *block* attackers from easy access to the system. In addition, a firewall can also monitor traffic leaving the system and can catch unusual activity like Trojan signals. However, not all are convinced that ICF is an effective safeguard against new threats.

"Microsoft Windows isn't exactly a shining example of an operating system that controls network shares (no operating system is, actually, but others are more configurable). On a monthly basis, messages are posted to security mailing lists describing new methods for getting around Windows security mechanisms." Siepmann, Frank. "SOHO Security Solutions". 3 April, 2000.

URL: <http://www.clothingtraining.org.hk/itlab/tips/tips1.htm>

In order to address all vulnerable components of this particular SOHO system, auditable safeguard controls must be in place. Moreover, these auditable controls must adhere to the current industry standards of information technology auditing methodologies. Some of these standards are COBIT (Control Objectives for Information & related Technology); FISCAM (Federal Information System Controls Audit Manual); and the more simplistic TBS (Time Based Security).

While COBIT and FISCAM frameworks are more commonly used by companies to develop security and compliance audits, since the *scope* of this audit is relatively less sophisticated than one for larger systems, I chose to use a mixed methodology of both Time and Compliance as dimensions to assess the system. These criteria are important to a system of this size, because while fairly easy to measure, they also address the variables that allow for the successful attacks (time) and secure configurations (compliance).

The principle idea of conducting an audit is to measure the current system against accepted security practices to determine the sufficiency of safeguards. This dictates the actions necessary for protection against critical risks and also determining the residual risks. Since acceptable levels of risk will differ between organizations, it is very important that the audit is conducted specifically for the environment under review. Therefore, my research also specifically addressed best practices for securing each of the vulnerable SOHO components.

There were lots of resources for Windows XP security issues to be found. The SANS Top 20 Internet Security Vulnerabilities was a good place to start to get a current list of the top twenty Microsoft Windows vulnerabilities. Not all were applicable, as they were not integral to the system, but there were several critical items that could not be overlooked. The proverbial 'horse's mouth' - Microsoft TechNet, website was another great source with the Microsoft Windows XP Security Guide Overview which helped in the compilation of the necessary services list. This list was not easy to do and must be maintained as changes are implemented. The Windows XP/2000 Answer Book also reinforced the

importance of hardening the O/S against exploits of known issues in its default state.

While the client would love to justify the investment of the cable modem, this investment is not based solely on its throughput efficiency, but also its defensive mechanisms. As mentioned before, cable modems have been widely believed to be insecure due to their shared media property; 'always on' network connection and the possibility of valid subscribers losing service to illegitimate users. It took some research to uncover that some of these beliefs may be unfounded.

The industry has come a long way and has reacted to both the privacy and security concerns with the DOCSIS specifications. However, while these specifications address the risks associated with the communication medium, there are still best practices that a cautionary user should adhere to – such as removing unnecessary services from the cable modem interface; running NAT (Network Address Translation) on a firewall; and physically unplugging from the modem when not in use. A comprehensive list of vulnerabilities and countermeasures can be found on the following website: TechRepublic, Facing the security risks of cable modems by James Michael Stewart. Other references worth mentioning are: The Cable Modem Reference Guide; Security in DOCSIS-based Cable Modem systems (See **References** for URLs).

Application security is becoming the greatest worry within the industry due to poorly written code or well written malware, depending on what side of the fence you are on. The threat, in this case, was less worrisome as the inventory of installed software was commercial and relatively small enough to monitor. Even though, the owner conducted e-commerce business transactions, it was via a web browser and not via an internal web server host.

Yet, there are inherent risks to transmitting any data over the Internet and with this client's type of business, and the sensitive nature of the daily web traffic makes it attractive to possible web application attacks. The web browser of choice is Microsoft Internet Explorer 6.0 which benefits from the automatic Windows Update feature in the XP platform. As soon as security updates are released by Microsoft, they are available on Windows Update and can be either automatically or manually installed.

Of course, one must throw caution to the wind, when it comes to enabling automatic software updates because of the uncertainty of the source. A good rule of thumb is to have a way to verify that it is a legitimate source and not a spoof attack. According to the Microsoft Security website, here are three ways to check:

- **The message contains no attachments.** Authentic Microsoft Security Bulletin notifications never include software updates as attachments. Rather, we refer customers to the complete version of the bulletin on our website, which provides a link to the update. Most Microsoft software updates are made through Microsoft® Windows® Update, Microsoft Office Update, or the Microsoft Download Center.

- **The message is digitally signed.** The Microsoft Security Response Center always signs its bulletin notifications before distributing them. You can verify the signature by using the key published on Microsoft TechNet.
- **The bulletin is listed on Microsoft.com.** We never send notices about security updates until after we publish information about them on our website. If you are ever in doubt about the authenticity of a Microsoft Security Bulletin notice, check TechNet to see if the bulletin is listed there

“How to Tell If a Microsoft Security-Related Message Is Genuine”

URL: http://www.microsoft.com/security/antivirus/authenticate_mail.asp

However, browser problems seem to be still prevalent because as recently as January 2004 another vulnerability was discovered for IE (versions 6 and below). The danger here is that a user can download what appears to be a safe text file whereas the file is actually an executable. “It is therefore only a matter of imagination in getting people to freely download what could be an extremely dangerous worm ... However what is more worrying...could easily be combined with another Explorer spoofing problem ...allowed Explorer users to think they were visiting one site when in fact they were visiting somewhere entirely different”.

McCarthy, Kieren. “New Explorer hole could be devastating”. Techworld.com.

28 January, 2004

URL: http://www.infoworld.com/article/04/01/28/HNiehole_1.html

Again, web application security best practices reinforce the idea of reconfiguring default states as in previous cases. Instead of being enabled by default (like other services), most of the security settings are actually disabled or minimally set. And, just like the operating system and other components, the optimum secure configuration differs from environment to environment.

What I found useful were unclassified guides published by the National Security Agency (NSA) government arm; Microsoft Security website and several other solid resources. Each reference had information that was not necessarily relevant to this standalone system that was still interesting to note. However, there were quite a few web security caveats that should not be overlooked in a sound audit checklist.

Web applications are riskier in nature in comparison to other installed applications since the data being manipulated is either in constant transit to a ‘trusted source’ or stored on a ‘trusted 3rd party server’. Therein lays the opportunity for an attack in multiple places.

Hardening the web browser means looking at the data (enabling SSL or TLS encryption, SHA-1 message digests); sender and receiver (enabling signed ActiveX digital signatures, checking for digital certificates revocation); web page contents (secure HTTPS instead of non-secure HTTP); privacy (cookie restrictions); embedded malicious scripts (disabling ActiveX, JavaScript or

VBScript); controlling user input and login procedures (eliminating overflows & SQL injections, enabling anti-caching and lock-out time periods).

This is an area that is presenting the most security risks these days and so it was not hard to find an abundance of research material. The Open Web Application Security Project (OWASP) is most comprehensive that I have found so far and its Top 10 2004 list of web application vulnerabilities is the U.S. Federal Trade recommended reference. These ten vulnerabilities are Invalidated Input; Broken Access Control; Broken and Session Management; Cross-Site Scripting (XSS) Flaws; Buffer Overflows; Injection Flaws; Improper Error Handling; Insecure Storage; Denial of Service; Insecure Configuration Management.

Of course, these are not all applicable to this particular environment. But it is enlightening to note that one particular vulnerability (Insecure Use of Cryptography) that was part of the Top 10 2003 list has now been removed. This is encouraging as it means that data protection has been better addressed in the implementation of the latest web application safeguards.

Part 2 – Create an Audit Checklist

This audit checklist is logically divided into the key components of the SOHO that were preliminarily assessed to be the most vulnerable – the O/S; Network/Cable Modem and Applications. Within each component, the items that comprised the checklist were prioritized by their **TFL (Threat Frequency Level > 10)**; **VF (Vulnerability Factor • 5)**; **IF (Impact Factor • 50** for the O/S, Applications, Operational, Physical/Environmental; • 27 for Network/Cable Modem as **Asset Values or AV** differ).

On the other hand, having a lower score for the variable **E (Effort < 5)** indicated that the **RF (Risk Factor)** would also be considerably lower. Therefore the items that made each checklist scored also > 2 for a **RF** in combination with other previously mentioned variables. Again, these variables were computed based on a quantitative formula based on reference material for industry best practices. In conjunction, I applied with a more subjective interpretation of these references based on personal experiences.

It is very important that the items that make this checklist verify not just the configurations of each tested component, but that the tested component behaves in the expected manner that assures that it is meeting the safety requirements. This fundamental element of safety must be evident (checked) and proven effective (against compliance criteria).

In a larger company, the auditor would probably start the process by first examining the current policies in place to see if they are implemented and enforced. These policies would maintain secure configuration of the system and

would cover a wide range from patch management, anti-virus updates, access control via firewall configurations and logs monitoring, passwords and accounts management, critical systems backups, incident response plans and disaster recovery, change management procedures.

The auditor would then use these policies and procedures to form an audit checklist. However, in this particular small company, such policies and procedures are non-existent. Therefore, baselining the system will have to be the initial step in order to compile information about it for future comparison.

Baselining has used frequently in the monitoring of IT systems to catch fluctuations from 'normal' states and this principle can be applied in IT auditing as well. Baselining not only measures the system, but it also provides a way to enforce procedures and identify critical areas where action should be taken.

For performance management purposes, baselining uses preset thresholds to indicate whether an error had occurred and some tools (like SNMP monitoring software) even offer notification to the appropriate parties. However, the scope for this audit is not merely utilization, but to identify critical items within each component whose known state need to be measured as any unusual activity may signal a potential compromise.

After a baseline snapshot of the system is created, an actual assessment will have to be carried out against it to ensure compliance. These will be more procedure and tool driven, but are important in determining how effective the safeguards (if in place) are and identifying areas where they should be implemented.

The references found in the earlier listed research material (from Part 1) also helped to define the scope of the audit and which key items should comprise each checklist. Just as importantly, these references also helped to provide a framework for developing testing procedures, compliance criteria and potential consequences for non-compliance.

Again, the scope has to be relative to the available environment and available resources to conduct the audit. Therefore each checklist contains checklist controls that assessed the not just the well-known risks in the industry, but only those that were present in this environment. An auditor that is assessing a similar platform in a multi-user, multi-machine, networked environment would probably choose to include other controls in his/her checklist.

2.1 – Operating System Audit Checklist

Checklist Control 2.1.1 - Checking for Default Installations	
Objective	To identify known issues such as open ports; unneeded services; unprotected accounts
Reference	<p>TFL = 20; VF = 9; IF = 90; E = 4</p> <ul style="list-style-type: none"> ➤ The SANS Top 20 Internet Security Vulnerabilities URL: http://www.sans.org/top20/ ➤ "HFNetChk 3.3 now Available". NTBugtraq. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind0201&L=NTBUGTRAQ&P=R2215&D=0&F=P&H=0&O=T&T=1 ➤ "What's new in Security for Windows XP Professional and Windows XP Home Edition". Microsoft TechNet. URL: http://www.microsoft.com/technet/prodtechnol/winxp/evaluate/xpsec.mspx ➤ Bradley, Tony. "Win2k Boot Disc Can Bypass Windows XP Passwords". Windows XP Security "Flaw". Internet/Network Security. About.com

	<p>URL: http://netsecurity.about.com/library/weekly/aa021603a.htm</p> <p>➤ "5- Minute Security Advisor: Essential Security Tools for Home Office and Power Users". Hardening Systems and Servers: Checklists and Guides. Microsoft TechNet. URL: http://www.microsoft.com/technet/security/topics/hardsys/default.msp</p> <p>➤ "Default settings for services". Microsoft Windows XP Home. URL: http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/WINDOWSXP/home/using/productdoc/en/sys_srv_default_settings.asp</p> <p>➤ "List of Services Needed to run a Secure IIS Computer". Microsoft Knowledge Base Article -189271. URL: http://support.microsoft.com/default.aspx?scid=kb:en-us:189271</p> <p>➤ "Description of Windows XP & Windows Server 2003 System File Checker". Microsoft Knowledge Base Article - 310747. URL: http://support.microsoft.com/default.aspx?scid=kb:EN-US:310747</p> <p>➤ "Security Basics for Home Users". Microsoft Security. URL: http://www.microsoft.com/security/home/</p> <p>➤ Microsoft Windows XP Security Guide Overview. Microsoft TechNet. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/winclnt/secwinxp/default.asp</p>
Risk	RF = 2.5
Testing Procedure/Tool	<p><u>1. Baseline the operating system to obtain a basic profile</u></p> <p>Tool: <i>System Tools</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Programs-> Accessories -> System Tools -> System Information</i></p> <p>(ii) <i>File -> Export -> XP_system_baseline</i> (export to both local drive & secondary storage disk)</p> <p>(iii) Note the important O/S values (O/S version; Total physical memory)</p> <p><u>2. Check for accounts (especially Administrator) and privileges established on O/S</u></p> <p>Tool: <i>User Accounts</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Control Panel -> User Accounts</i></p> <p>(ii) Note the number of accounts established</p> <p>(iii) Click on each account; Note password existence and type of privilege</p> <p>(iv) Click on <i>Change an account; Pick an account to change</i>; Disable <i>Guest</i>; Assign appropriate privileges (<i>Computer Administrator</i> or <i>Limited Account</i>) & password protection to each valid account; Delete invalid accounts (<i>Change an account</i>; Click on invalid account; <i>Delete the account</i>)</p> <p><i>Service Accounts</i></p> <p><u>3. Check for running services</u></p> <p>Tool: <i>Administrative Tools</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Control Panel -> Administrative Tools -> Services</i></p> <p><u>4. Scan for open ports (to verify what services are on which port)</u></p> <p>Tool: <i>NeWT.exe Nessus Windows Technology</i> vulnerability scanner (External scans)</p> <p>Procedure:</p> <p>(i) <i>Start -> Programs -> Tenable NeWT -> NeWT Security Scanner</i></p> <p>(ii) From the menu choose <i>Configure NeWT</i>; Under the <i>General</i> tab, change <i>Max number of hosts</i> to <i>1</i>; Change <i>Port range to scan</i> from <i>Default</i> to <i>0-65535</i>; Check <i>Auto-enable dependencies</i>; Check <i>Optimize test</i>.</p> <p>(iii) Under the <i>Ping</i> tab, Check <i>Do a TCP ping</i>; Check <i>Do an ICMP ping</i></p> <p>(iv) From the menu choose <i>New Scan Task</i>; Under <i>Please enter the target you want to scan</i>, enter the hostname or IP address of the system (you can also import the target from a file as well).</p> <p>(v) Under <i>Please choose the plugins set you want to use</i>; Select <i>Use a predefined plugin set</i></p> <p>(vi) Select <i>Next</i>; Choose <i>Port Scan</i> and <i>Scan now</i></p> <p>(vii) <i>File -> Save as</i>; To save the HTML report of the port scan results</p> <p>Tool: <i>netstat.exe</i> utility (Internal scans)</p> <p>Procedure: <i>Start -> Run -> netstat-na</i></p> <p><u>5. Determine necessary services</u></p> <p>Tool:</p> <p>(i) Research each service to see if necessary by comparison to system's intended role</p> <p>(ii) Use published guides from <i>Microsoft Knowledge Base</i> articles & double check with the client/administrator of the system</p> <p>(iii) The following services were deemed unnecessary (<i>Alerter; Application Management; ClipBook; COM+ System Application; Distributed Transaction Coordinator; Messenger; Net Logon; Net Meeting Remote Desktop Sharing; Network DDE & DSDM; Remote Desktop Help Session Manager; Remote Packet Capture Protocol v.0; RPC Locator; Routing and Remote Access; TCP/IP NetBIOS Helper</i>)</p>

	<p>Procedure:</p> <p>(i) <i>Start -> Control Panel -> Administrative Tools -> Services</i></p> <p>(ii) Double click on each service listed above; Go to <i>General</i> tab; From <i>Startup Type</i> drop-down menu select <i>Disable</i>; <i>OK</i>.</p> <p><u>6. Check share permissions</u></p> <p>Tool: <i>Administrative Tools</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Control Panel -> Administrative Tools -> Computer Management-> Shared Folders -> Shares</i></p> <p>(ii) Check for non special systems shares like folders, printers</p> <p><u>7. Check critical registry settings</u></p> <p>Tool: <i>Registry Editor</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Run -> regedit</i></p> <p>(ii) Right click on <i>HKEY_LOCAL_MACHINE -> Permissions</i>; Check list of for appropriate <i>Groups or Users</i>; Click on <i>Delete</i> or <i>Add</i> to change; within <i>Groups or Users</i> & assign appropriate permissions - <i>Full Control, Read, Special Permissions</i></p> <p>(iii) Right click on <i>HKEY_LOCAL_MACHINE -> System -> CurrentControlSet -> Control -> Lsa</i>; Right click on value <i>noLmhash</i>; <i>Modify</i> to <i>1</i> to disable storage of weak LM password hashes</p> <p><u>8. Check file systems</u></p> <p>Tool: <i>System File Checker</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Run -> Sfc /scanboot</i></p> <p><u>9. Manage logging of critical events for an audit trail</u></p> <p>Tool: <i>Administrative Tools</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Control Panel ->Administrative Tools -> Event Viewer -> Security</i></p> <p>(ii) Check the <i>Category</i> column for critical events – <i>System Event; Logon/Logoff; Account Logon</i></p> <p>(iii) Check the <i>Type</i> column for failed & successful events for unusual activity</p> <p>(iv) Right click on <i>Security -> Properties</i>; Increase <i>Maximum log size >10 MB</i>; <i>Overwrite events over than 7 days</i></p> <p>Procedure:</p> <p>(i) <i>Start -> Control Panel ->Administrative Tools -> Event Viewer -> System</i></p> <p>(ii) Check the <i>Type</i> column for system events ranging in severity from <i>Information; Warning; Error</i></p> <p>(iii) Right click on <i>System -> Properties</i>; Increase <i>Maximum log size >10 MB</i>; <i>Overwrite events over than 7 days</i></p> <p><u>10. Check to see if built-in firewall (ICF) is enabled</u></p> <p>Tool: <i>Network Connections</i></p> <p>(i) <i>Start -> Control Panel -> Network Connections</i>; Right click appropriate connection icon; Click on <i>Properties -> Advanced</i> tab; <i>Enable Internet Connection Firewall</i></p>
Compliance Criteria	<p><u>1. Baseline:</u></p> <p>Compliance check:</p> <p>(●) Copy of baseline info must resident on secondary storage media (CD-R)</p> <p><u>2. Accounts</u></p> <p>Compliance check:</p> <p>(●) Only one account must be configured with administrator privileges</p> <p>(●) All accounts must be password protected</p> <p>(●) The <i>Guest</i> account must be disabled</p> <p><u>3. Services & Ports</u></p> <p>Compliance check:</p> <p>(●) Only essential services (from compiled list) are to be set as automatic startup</p> <p>(●) Port scan to verify that the services listening on open ports are on compiled list.</p> <p><u>4. Shares</u></p> <p>Compliance check:</p> <p>(●) Remove any special systems shares like folders, printers; The only permissible shared object should be <i>\$IFC</i> .</p> <p><u>5. Weak Password Protection</u></p> <p>Compliance check:</p> <p>(●) The value of the <i>noLmhash</i> registry key should be set to <i>1</i> which disables the storage of weak LM password hashes.</p> <p><u>6. File System Integrity</u></p> <p>Compliance check:</p> <p>(●) The value of the <i>SfcScan</i> DWORD should be set to <i>1</i> which forces the system to scan all protected system files at reboot.</p> <p><u>7. Audit trails</u></p> <p>Compliance check:</p>

	<p>(●) Critical events (such as <i>System Event; Logon/Logoff; Account Logon</i>) must be written to a log file of at least 10MB and kept for 7 days.</p> <p>8. Firewall</p> <p>Compliance check:</p> <p>(●) The internal firewall port blocking mechanism (<i>IFC</i>) must be checked to be enabled because it is disabled by default.</p>
Test Nature	Subjective (Control 5) Objective (Controls 1-4, 6-10)
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)
Checklist Control 2.1.2 - Checking for Unpatched Systems	
Objective	To address known issues such as exploitable vulnerabilities; faulty code
Reference	<p>TFL = 45; VF = 9; IF = 90; E = 2</p> <ul style="list-style-type: none"> ➤ The SANS Top 20 Internet Security Vulnerabilities URL: http://www.sans.org/top20/ ➤ "Hardening Systems and Servers: Checklists and Guides". Microsoft TechNet. http://www.microsoft.com/technet/security/topics/hardsys/default.mspix ➤ Microsoft Baseline Security Analyzer, Windows Update. URL: http://v4.windowsupdate.microsoft.com/en/default.asp ➤ "5 Minute Security Advisor – Essential Security Tools for Home Office Users". First Things First ... MBSA. Microsoft TechNet. URL: http://www.microsoft.com/technet/community/columns/5min/5min-105.mspix#XSLTsection125121120120 ➤ NTBugtraq. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=38&sid=1
Risk	RF = 5
Testing Procedure/Tool	<p>1. Check system for current patch level:</p> <p>Tool: <i>Microsoft Baseline Security Analyzer (MBSA) v 1.2 (hfnetchk.exe)</i></p> <p>Procedure:</p> <p>(i) Click on URL: http://windowsupdate.microsoft.com to run an automatic <i>Windows Update</i></p> <p>(ii) Click on <i>Scan for updates</i></p> <p>(iii) Save the results to a text file</p> <p>(iv) Use this scan results list to check for possible missing critical patches</p> <p>(v) If critical missing patches are noted, then back up system with a zip drive and then proceed with the required patches installation</p> <p>(vi) Within the <i>Windows Update</i> window, click on <i>Review & install updates</i></p> <p>(vii) Choose <i>Add</i> for the updates that are required</p>
Compliance Criteria	<p>1. Required Patches</p> <p>Compliance check:</p> <p>(●) Must install all patches for <i>Microsoft XP</i> [Version 5.1.2600]; Use <i>MBSA</i> report to see if all missing critical updates are added</p> <p>2. Automatic Patch Updating:</p> <p>Compliance check:</p> <p>(●) Must install an automatic agent for patch management; Check <i>System Properties (Start -> Control Panel -> System Properties -> Automatic Updates</i>; Verify that <i>Keep my computer up to date & Download automatically and notify me when they are ready to be installed</i> are enabled.</p>
Test Nature	Objective/Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)
Checklist Control 2.1.3 - Checking for Outdated Virus Definitions	
Objective	To address having sufficient protection against known and future malware
Reference	<p>TFL = 45; VF = 9; IF = 90; E = 2</p> <ul style="list-style-type: none"> ➤ "Security Basics for Home Users". Microsoft Security. URL: http://www.microsoft.com/security/home/ ➤ "5 Minute Security Advisor – Essential Security Tools for Home Office Users - Virus Scanners". Microsoft TechNet. URL: http://www.microsoft.com/technet/community/columns/5min/5min-105.mspix#XSLTsection125121120120
Risk	RF = 5

Testing Procedure/Tool	1. Check for antivirus software Tool: Look for any commercial anti-virus software Procedure: (i) <i>Start-> Programs</i> (Look for Symantec Norton Antivirus 2003; McAfee Virusscan 8.0; etc.,) (ii) If installed, double click to run an update
Compliance Criteria	1. Antivirus Software: Compliance check: (●) Must have antivirus software installed (commercial preferred); Check list of installed software for commercial products like Symantec Norton Antivirus 2003; McAfee Virusscan) 2. Automatic Virus Definitions Updating: Compliance check: (●) Must keep subscription current for virus definition updates; Check subscription to see if current.
Test Nature	Objective/Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)

2.2 – Network/Cable Modem Audit Checklist

Checklist Control 2.2.1 - Checking for Perimeter Penetration	
Objective	To determine if defense-in-depth is needed to counter against a single point of failure (or whether the O/S firewall –IFC & security features of the DOCSIS cable modem are sufficient)
Reference	TFL = 20; VF = 9; IF = 90; E = 4 <ul style="list-style-type: none"> ➤ Bradley, Tony. "Security Basics At Home". Internet/Network Security. About.com URL: http://netsecurity.about.com/library/weekly/aa011003a.htm ➤ Questions and Answers: Security 1.2. The Cable Modem Reference Guide. Cable-Modems.org. URL: http://www.cable-modems.org/q&a/#1.2 ➤ "How big an issue is security for the Internet, broadband and my computer?". Getting Connected: Security. Cable-Modems.net. URL: http://www.cable-modem.net/gc/security.html ➤ Stewart, M. James. "Facing the security risks of cable modems". 8 July, 2002. ZDNet UK. URL: http://insight.zdnet.co.uk/hardware/servers/0.39020445.2118716.00.htm ➤ "Security in DOCSIS-based Cable Modem systems". Section 2: Security of Data Transport Services. Page 2. URL: http://www.cablemodem.com/downloads/Security_in_DOCSIS.pdf ➤ McKelvey, T. Joel. Cisco Systems, Inc., USA. "Combating security risks on the cable IP network". URL: http://www.broadcastpapers.com/broadband/IBCCiscoSecurityCableIP01.htm ➤ Microsoft Security. "Security Basics for Home Users". URL: http://www.microsoft.com/security/home/ ➤ Wolfblade. "Windows XP Internet Connection Firewall. GameSpy Arcade [HELP]ers URL: http://www.gamespyarcade.com/helpers/workshop/xpfirewall/ ➤ Weigel, Ray. " Windows XP comes packed with a down and dirty firewall". Inside XP: Internet Connection Firewall. Products and Reviews. 30 September, 2001. Techtv. URL: http://www.techtv.com/products/software/story/0.23008.3338448.00.html ➤ "How to manually open ports in the Windows XP Internet Connection Firewall". Protect your PC. 7 November, 2003. Microsoft Security. URL: http://www.microsoft.com/security/protect/ports.asp
Risk	RF = 2.5
Testing Procedure/Tool	1. NETWORK 1. Reconnaissance/Gather footprint info Tool: <i>ping.exe</i> utility to see what information the system responds with Procedure: (ii) <i>Start -> Run -> ping -a xxx.xxx.xxx.xxx</i> (Resolves the IP address to hostname) (iii) <i>Start -> Run -> ping -n 4 xxx.xxx.xxx.xxx</i> (Test to see if it allows 4 incoming echo request packets) 2. Check for possible perimeter vulnerabilities (Zero Knowledge Test) Tool: <i>NeWt.exe</i> <i>Nessus Windows Technology</i> incorporates other utility checks – including <i>nmap</i> . (Remember to obtain prior approval before proceeding to scan system) Procedure: (i) <i>Start -> Programs -> Tenable NeWT -> NeWT Security Scanner</i>

- (ii) From the menu choose *Configure NeWT*; Under the *General* tab, change *Max number of hosts* to *1*; Change *Port range to scan* from *Default* to *0-65535*; Check *Auto-enable dependencies*; Check *Optimize test*.
- (iii) Under the *Ping* tab, Check *Do a TCP ping*; Check *Do an ICMP ping*
- (iv) Under the *Login* tab, verify that anonymous FTP is included in scan
- (v) From the menu choose *New Scan Task*; Under *Please enter the target you want to scan*, enter the hostname or IP address of the system (you can also import the target from a file as well).
- (vi) Under *Please choose the plugins set you want to use*; Select *Use a predefined plugin set*
- (vii) Select *Next*; Choose *Port Scan* and *Scan now*
- (viii) *File -> Save as*; To save the HTML report of the port scan results
- (ix) Repeat (i-iii); Select *Next*; Choose *SANS TOP 20* and *Scan now*
- (x) *File -> Save as*; To save the HTML report of the SANS TOP 20 vulnerabilities scan results
- (xi) Select *Next*; Choose *SOHO_Scan_1()* and *Scan now*
- (xii) Repeat (i-iii); Select *Next*; Choose *SOHO_Scan_1()* and *Scan now*
- (xiii) *File -> Save as*; To save the HTML report of the SOHO vulnerabilities scan results

3. Check the exploitability of these holes

Tool:

NeWt.exe (*Nessus Windows Technology*; Use plugins for more advanced & customized in depth scan & penetration testing)

Procedure:

- (i) First obtain written consent from responsible parties and inform parties of the specific start time and estimated duration of penetration testing period.
- (ii) Test remote access with connectivity protocols – (For e.g., telnet, rpc, ftp)
Under *Please choose the plugins set you want to use*; Select *Define my own set of plugins*;
Select plugins to use – by Families
(Note: Always check: *Do not use dangerous plugins even if they are selected*).
Check *Backdoors* & keep all the default *plugins*; *Start scan now*
Check *Denial of Service* & keep all the default *plugins*; *Start scan now*
Check *FTP* & uncheck UNIX-related *plugins* (For e.g., AIX, Linux, HPU-UX, Sun); *Start scan now*;
Check *RPC* & check only Windows-related *plugins* (For e.g., database service, RPC portmapper, snmp service, X25 service); *Start scan now*
Check *Useless Services* & uncheck UNIX-specific daemons (e.g., *rlogin*, *rsh*; *telnet* should be enabled); *Start scan now*
- (iii) Test other services/vulnerabilities by selecting other *Families* of plugins
Check *Windows* & uncheck components not specific to this environment (e.g., *SQL*, *CA Unicenter*); *Start scan now*
Check *Windows User Management* & uncheck components not specific to this environment (e.g., *Users* in different groups other than *Admin*); *Start scan now*
Check *Peer to Peer File Sharing* & uncheck components not specific to this environment (e.g., *Web Server* & *FTP Server hosting*); *Start scan now*
Check *Firewalls* & uncheck other vendor hardware plugins as this environment is using the built-in software firewall – *IFC* (e.g., *Checkpoint*, *Raptor*, *PIX*, *BenHur*, *Kerio*, *IBM* & *StoneGate*); *Start scan now*

4. Harden network by plugging holes

Tool:

Nessus reports

Procedure:

- (i) *Start -> Programs -> Tenable NeWT -> NeWT Security Scanner*
- (ii) From the menu choose *View Reports*; Under *Select a report to view*, double click on report
- (iii) Go over the results of each type of scan and follow the recommended solutions to any critical holes or less serious informational notes found.

Tool:

Network Connections

Procedure:

- (i) *Start -> Control Panel -> Network Connections*
- (ii) Under *LAN or High Speed Internet* right click on enabled *Local Area Connection* icon
- (iii) Click on *Properties -> Advanced -> Settings*;
- (iv) Under the *Services* tab first uncheck each of the unnecessary connectivity services – *FTP*, *Telnet*; Next uncheck other unneeded services (per previous research)
- (v) Under the *Security Logging* tab, check *Log dropped packets* & *Log successful connections* to enable firewall logging
- (vi) Under *ICMP* tab, uncheck *Allow incoming echo request*; *Allow incoming mask request*; *Allow outgoing destination unreachable*; *Allow outgoing source quench*; *Allow redirect* – so that these messages will be blocked.
- (vii) Under the *Authentication* tab, check *Enable network access control using IEEE 802.1X* for appropriate *EAP* type; check *Authenticate as computer when computer information is available*
- (iii) Under the *General* tab uncheck *File and Printer Sharing for Microsoft Networks*

5. Review firewall logs for suspicious activity

Tool:

Notepad text editor

Procedure:

- (i) See above to access the *Security Logging* tab;
- (ii) Under *Log file options*, in *Name*, click *Browse*.
- (iii) Scroll to the *ICF* security log; right-click the file -> *Open*

	<p>CABLE MODEM</p> <p>1. Check SNMP configurations</p> <p>Tool:</p> <p>After thorough research, it was discovered that unfortunately, only the cable provider and not the subscriber can access the modem directly to check these configurations.</p> <p>Procedure:</p> <p>(i) Check with ISP to see if they are aware of the <i>SNMP</i> security implications & have taken the necessary steps to circumvent them (For e.g., <i>Public community string</i> must be set to <i>READONLY</i> to prevent unauthorized remote manipulation)</p> <p>(ii) From the subscriber's end, the <i>SNMP</i> agent can be disabled (if system is a server) via <i>Control Panel -> Administrative Tools -> Services</i>; Right click on <i>SNMP</i> service; <i>Stop</i>. On a standalone machine, as in this case, <i>SNMP</i> (Ports <i>161</i>, <i>162</i>) should not be established.</p> <p>To check: <i>Start -> Run -> netstat -na</i></p> <p>2. Check to see if sharing is turned off</p> <p>Tool:</p> <p>Procedure:</p> <p>(i) Check with ISP to see if they are aware of the file sharing security implications & have taken the necessary steps to circumvent them (For e.g., <i>Internet Connection Sharing</i>)</p> <p>(ii) From the subscriber's end, network sharing can be disabled via <i>Start -> Control Panel -> Network Connections</i>; Under <i>LAN or High Speed Internet</i> right click on enabled <i>Local Area Connection</i> icon; Under the <i>General</i> tab uncheck <i>File and Printer Sharing for Microsoft Networks</i></p> <p>3. Check to see if modem DOCSIS compliant for support of BPI & BPI+</p> <p>Tool:</p> <p>Check Toshiba PCX2500 online manual for specifications.</p> <p>Procedure:</p> <p>Click on URL: http://www.toshiba.com/taisnpd/products/pcx2500.html</p> <p>4. Check for installed Symantec's Norton Internet Security™ 2004 protection</p> <p>Tool:</p> <p>Check Toshiba PCX2500 online manual for specifications.</p> <p>Procedure:</p> <p>Click on URL: http://www.toshiba.com/taisnpd/products/pcx2500.html</p>
Compliance Criteria	<p>NETWORK</p> <p>1. Reconnaissance check (Limit publicized info of non-critical items; Limit system responses)</p> <p>Compliance check:</p> <p>(●) Limit <i>ICMP</i> (Deny IP direct broadcasts; unreachable messages; echo requests)</p> <p>2. Acceptable open ports</p> <p>Compliance check:</p> <p>(●) Use earlier compiled list</p> <p>3. Allowed protocols</p> <p>Compliance check:</p> <p>(●) <i>ICF</i> firewall rules should deny everything else not on list.</p> <p>(●) If in the future, more services need to be turned on (e.g., file sharing for a specific computer added to the office), then add specific port:</p> <p>(i) <i>Start -> Control Panel -> Network Connections</i></p> <p>(ii) Under <i>LAN or High Speed Internet</i> right click on enabled <i>Local Area Connection</i> icon</p> <p>(iii) Click on <i>Properties -> Advanced -> Settings -> Add</i> to open a new port; <i>Type in Description of Service; Name or IP Address of computer; 445</i> for both External & Internal Port numbers; <i>TCP</i> or <i>UDP</i></p> <p>4. Firewall logging enabled</p> <p>Compliance check:</p> <p>(●) Firewall events must be logged; To verify access <i>Local Area Connection</i> icon (see above); Click on <i>Properties -> Advanced -> Settings</i>; Go to <i>Security Logging</i> tab & verify under <i>Logging options - Log dropped packets; Log successful connections</i> are checked.</p> <p>CABLE MODEM</p> <p>1. SNMP Access:</p> <p>Compliance check:</p> <p>(●) <i>Public community string</i> must be set to <i>READONLY</i> (Verify with cable service provider)</p> <p>2. File Sharing:</p> <p>Compliance check:</p> <p>(●) Must disabled this service as it is known to be enabled by default (by enabling <i>ICF</i>)</p> <p>(●) Filter firewall traffic on <i>UDP/TCP</i> ports <i>137 -139</i> to block Microsoft Windows <i>SMB/NBT</i> file sharing (in case an older Microsoft machine running Windows 95,98 or NT is later added to the office & uses NetBIOS or System Message Block file sharing protocols for shared system resources)</p> <p>3. DOCSIS Compliant: Eliminates possibility of IP broadcasting; Offers security & privacy features</p> <p>Compliance check:</p> <p>(●) Check specifications for this particular model – PCX2500</p> <p>4. Physically disconnect equipment :</p>

	Compliance check: (●) Unplug modem when not in use to reduce window of opportunity
Test Nature	Objective/Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)

2.3 – Application Audit Checklist

Checklist Control 2.3.1 - Checking for Checking for Faulty Installations	
Objective	To avoid compromising the system w/default or unknown source installations
Reference	TFL = 25; VF =7; IF = 70; E = 2 <ul style="list-style-type: none"> ➤ The SANS Top 20 Internet Security Vulnerabilities URL: http://www.sans.org/top20/ ➤ "HFNetChk 3.3 now Available". NTBugtraq. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind0201&L=NTBUGTRAQ&P=R2215&D=0&F=P&H=0&O=T&T=1 ➤ "Security Basics for Home Users". Microsoft Security. URL: http://www.microsoft.com/security/home/
Risk	RF = 5
Testing Procedure/Tool	1. Obtain software profile Tool: <i>Add or Remove Programs</i> Procedure: <i>Start -> Control Panel -> Add or Remove Programs</i> 2. Check list for new or unknown installations Tool: <i>Add or Remove Programs</i> Procedure: Use scroll bar to move up and down list 3. Remove suspect or unused programs Tool: <i>Add or Remove Programs</i> Procedure: <i>Start -> Control Panel -> Add or Remove Programs; Click on Sort by for drop-down menu; Sort by Frequency of use; Click on software and select Remove unwanted or suspect software</i>
Compliance Criteria	1. New Software Notification: Compliance check: (●) Feature to notify/approve of new installations enabled by default in Windows XP
Test Nature	Objective/Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)
Checklist Control 2.3.2 - Checking for Unknown Downloads	
Objective	To avoid compromising the system with attachments that contain malware
Reference	TFL = 45; VF =9; IF = 90; E = 2 <ul style="list-style-type: none"> ➤ The SANS Top 20 Internet Security Vulnerabilities URL: http://www.sans.org/top20/ ➤ "HFNetChk 3.3 now Available". NTBugtraq. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind0201&L=NTBUGTRAQ&P=R2215&D=0&F=P&H=0&O=T&T=1 ➤ "Security Basics for Home Users". Microsoft Security. URL: http://www.microsoft.com/security/home/ ➤ Seltzer, Larry. "Fresh Worms Attack E-mail, Internet Explorer, User Data". 25 February 2004. eWeek Enterprise News & Reviews. URL: http://www.eweek.com/article2/0.1759.1538954.00.asp ➤ Outlook Email Security Update. 19 February 2004. Slipstick Systems. URL: http://www.slipstick.com/outlook/esecup.htm ➤ "Help protect your Inbox from email viruses". Security features for Outlook 2002 and previous versions. 26 April, 2002. Microsoft Office Online. URL: http://www.microsoft.com/office/previous/outlook/2002security.asp
Risk	RF = 5
Testing	1. Check to see if using Outlook 2002 for an email software which has download

Procedure/Tool	restrictions configurations Tool: (i) <i>Start -> Programs -> Microsoft Office</i> (ii) From menu, click on <i>Help; About Microsoft Office</i> (for version)
Compliance Criteria	1. Email software must automatically restrict certain executable attachments: Compliance check: (●) Must be running at least Microsoft Outlook 2002 or if earlier version (must have security patches)
Test Nature	Objective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)
Checklist Control 2.3.3 - Checking for Outdated Virus Definitions	
Objective	To avoid compromising the system w/default or unknown source installations
Reference	TFL = 8.75; VF = 7; IF = 70; E = 2 <ul style="list-style-type: none"> ➤ Microsoft Security. "Security Basics for Home Users". URL: http://www.microsoft.com/security/home/ ➤ Microsoft TechNet. "5 Minute Security Advisor – Essential Security Tools for Home Office Users" Virus Scanners. URL: http://www.microsoft.com/technet/community/columns/5min/5min-105.msp#XSLTsection125121120120
Risk	RF = 5
Testing Procedure/Tool	1. Check for antivirus software Tool: Any commercial anti-virus software (For example, Norton Antivirus 2003; McAfee Virusscan 8.0) Procedure: (i) <i>Start-> Programs</i> (Look for Norton Antivirus 2003; McAfee Virusscan 8.0; etc.,) (ii) If installed, double click to run an update
Compliance Criteria	1. Antivirus Software: Compliance check: (●) Must have antivirus software installed (commercial preferred); Check list of installed software for commercial products like Norton Antivirus 2003; McAfee Virusscan) 2. Automatic Virus Definitions Updating: Compliance check: (●) Must keep subscription current for virus definition updates; Check subscription to see if current.
Test Nature	Objective/Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)
Checklist Control 2.3.4 - Checking for Weak Protection of Sensitive Data	
Objective	To avoid improper info disclosure and/or alteration of data
Reference	TFL = 35; VF = 7; IF = 70; E = 2 <ul style="list-style-type: none"> ➤ "Security Basics for Home Users". Microsoft Security. URL: http://www.microsoft.com/security/home/ ➤ "Using Office Security features". 9 March, 2004. Microsoft Security URL: http://www.microsoft.com/security/articles/officesec.asp ➤ "5 Minute Security Advisor – Essential Security Tools for Home Office Users" . Virus Scanners. Microsoft TechNet. URL: http://www.microsoft.com/technet/community/columns/5min/5min-105.msp#XSLTsection125121120120 ➤ "Improving Web Application Security: Threats and Countermeasures". Microsoft TechNet, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp ➤ McCarthy, Kieren. "New Explorer hole could be devastating". Techworld.com. 28 January, 2004 URL: http://www.infoworld.com/article/04/01/28/HNehole_1.html ➤ "Understand and maintain security with Internet Explorer". Microsoft Internet Explorer Home. 22 October 2003. URL: http://www.microsoft.com/windows/ie/security/default.asp ➤ "Which versions of Internet Explorer are Affected by Security Issues?". Internet Explorer Security Issues. Microsoft Internet Explorer Security Center. URL: http://www.nwnetworks.com/iesecurity.htm ➤ Doernberg, Curt. "Guide to Securing Microsoft Internet Explorer 5.5 Security Using Group Policy". National Security Agency Security Recommendation Guides. Version 1.0. July 2002. URL: http://nsa2.www.conxion.com/support/guides/sd-8.pdf

Risk	RF = 5
Testing Procedure/Tool	<p>1. Check browser settings for secure configurations: Tool: Microsoft Internet Explorer 6.0 Procedure: (i) Start-> Program -> Microsoft Internet Explorer (ii) Tools -> Internet Options (iii) Click on the <i>Security</i> tab, Click on <i>Custom Level</i> button; (iv) <i>Disable</i> the following settings: <i>Download unsigned ActiveX controls, Initialize and script ActiveX controls not marked as safe, Access data sources across domains, Don't prompt for client certificate when no certificates or only one certificate exists; Downloads, File download</i> (v) For <i>User Authentication, Logon</i>, Click on <i>Prompt for user name and password</i> (vi) Click on the <i>Privacy</i> tab, Move slider all the way to the top to on <i>Block All Cookies</i> (vii) Click on the <i>Content</i> tab, click on <i>Certificates</i> to import them into a single store (viii) Click on the <i>Advanced</i> tab, scroll down to <i>Security</i> and check to enable the following: <i>Check for publisher's certificate revocation; Check for server certificate revocation, Check for signatures on downloaded programs, Empty Temporary Internet Files folder when browser is closed, Enable Integrated Windows Authentication, Enable Profile Assistant, Use SSL 2.0, Use SSL 3.0, Use SSL 1.0, Use TLS 1.0, Warn about invalid site certificates, Warn if changing between secure and not secure mode, Warn if forms submittal is being directed.</i></p> <p>2. Check Office applications for secure configurations: Tool: Microsoft Office 2003 applications (Word, Excel, PowerPoint, etc) Procedure: (Read-only protection) (i) Open file; Tools -> Options -> Security; (ii) In <i>Password to modify</i>, type a password; OK (iii) In <i>Reenter password to modify</i>; type password again; OK Procedure: (Password protection) (i) Open file; Tools -> Options -> Security; (ii) In <i>Password to open</i>; type a password; OK (iii) In <i>Reenter password to modify</i>; type password again; OK</p>
Compliance Criteria	<p>1. Secure browser configurations: Compliance check: (●) Configurations must adhere to checklist outlined in Testing Procedure 2. Secure Office applications Compliance check: (●) Office files must be password protected 3. Automatic Virus Definitions Updating: Compliance check: (●) Must keep have a current subscription for an anti-virus software virus. 3. NeWT Plugin: Compliance check: (●) Must have 0 vulnerabilities</p>
Test Nature	Objective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)

2.4 – Operational Audit Checklist

Checklist Control 2.4.1 - Checking for Data Retention Protection	
Objective	To make sure mechanisms are in place to prevent data loss (physically & electronically)
Reference	<p>TFL = 15; VF = 5; IF = 50; E = 2</p> <ul style="list-style-type: none"> ➤ LiveVault Online Backup and Recovery. U.S. Small Business Administration. "Backup and Recovery: Keeping it Simple for Small Business". URL: http://www.livevault.com/customers/service_success/sba.asp ➤ Enbysk, Monte. SmallTech. "Lost data can cripple your business". URL: http://www.bcentral.com/articles/enbysk/125.asp?format=print ➤ Fusco, Patricia. Small Business Computing.Com. "Backup and recovery systems designed for SMBs". 7 February, 2003. URL: http://www.smallbusinesscomputing.com/biztools/article.php/1580901
Risk	RF = 5
Testing Procedure/Tool	<p>1. Check for backup mechanisms in place Tool/Procedure: (i) Local removable backup media (Zip/Jaz/CD-R) and compress to an archive for storage</p>

	(ii) Using a traditional client-server backup software on a spare standalone system (For e.g., <i>Backup for Workgroups 1.0</i> allows powerful backup & restoration on a system of at least 150MB) (iii) Subscription to a vendor for remote storage services 2. Check whether backup data is stored on-site or off-site (data vaulting) Tool/Procedure: (i) Interview client/administrator (Only necessary if using local backup media)
Compliance Criteria	1. Acceptable backup mechanism in place Compliance check: (●) A zip drive with a capacity of 750MB (e.g., Iomega or comparable backup mechanism) 2. Acceptable off-site data storage location Compliance check: (●) A reputable company that provides data vaulting services –vital in recovering critical data 3. Acceptable retention period (for SEC and IRS) Compliance check: (●) Since the data is financial in nature, it is subject to retention of records relevant to Audits and Reviews, Securities and Exchange Commission, 17 CFR Part 210; and IRS procedure 86-19
Test Nature	Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)

2.5 – Physical/Environmental Audit Checklist

Checklist Control 2.5.1 - Checking for Sufficient Fire Detection/Suppression	
Objective	To make sure mechanisms are in place to prevent physical destruction by fire
Reference	TFL = 13.5; VF = 5; IF = 50; E = 2 ➤ Krutz, L Ronald. Vines, D. Russell. <i>The CISSP Prep Guide: Gold Edition</i> . Indianapolis: Wiley Publishing, Inc., 2003, Pages 469-472
Risk	RF = 4.5
Testing Procedure/Tool	1. Check for smoke detector & working batteries 2. Check for fire extinguisher
Compliance Criteria	1. Smoke Detector & working batteries Compliance check: (●) A working smoke detector in the office area 2. Fire extinguisher Compliance check: (●) A working fire extinguisher in office area
Test Nature	Subjective
Evidence	Determined in Part 3 (Actual Audit)
Findings	Determined in Part 3 (Actual Audit)

Part 3 – Conduct the Audit – Testing, Evidence and Findings

Each key component of the SOHO will now be tested against the audit checklist to see if its configuration is as secure as it should be. Each checklist item was carefully chosen as the best control or method to test for a given risk possibly present in one of the components. To test for the presence of a risk, one has to see if any of the known vulnerabilities can be exploited and this involves a stimulus/response to clearly prove its behavior. The idea is to gain confidence in safeguards in place and identify areas where they may be needed.

This particular system has no security policies in place nor adhered to any best practices followed by small offices running similar systems. Efficiency was the business' motto and security was an after-thought. Therefore as this audit is approached, it is expected that there will be many improvements needed to bring the system into compliance with the recommended secure configurations. For auditors of larger systems, a feasible approach to this very labor-intensive problem is to find an automated software package that comprehensively evaluates the system against standards, e.g., (BS 7799, ISO 17799) or regulations like (HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley) and generates a customized solution.

The approach utilized here is manual and although time consuming, the environment is small enough to justify the method. With a collection tools – built-in Windows system utilities; reconnaissance and vulnerability scanning security tools; and research references of industry best practices, an audit of this scope can be accomplished.

The aim of the compliance criteria is to enforce the best practices of security controls for critical vulnerabilities found for the components of this SOHO. The idea, again, is to remove the vulnerabilities as threats will always be present and there is not much one can do to change that. Threat + Vulnerability = Risk. The desired result is risk mitigation – which can either be reduction, transference and/or acceptance. The findings of the audit will dictate what the necessary steps should be.

3.1 – Operating System Audit Results

Checklist Control 3.1.1 - Checking for Default Installations	
Objective	To identify known issues such as open ports; unneeded services; unprotected accounts
Evidence	<ul style="list-style-type: none">▪ Appendix A - XP_system_baseline (excerpt of file)▪ Appendix B - Snapshot of Local Services Running▪ Appendix C - Nessus Port Scan Results (External)▪ Appendix D - Netstat Port Scan Results (Internal)▪ Appendix E - Allowable Share Permissions▪ Appendix F - Lan Manager Registry Settings▪ Appendix G - Microsoft Internet Connection Firewall▪ Appendix H - User Accounts
Findings	Items in Compliance: <ul style="list-style-type: none">• Allowable Share Permissions (No folders or printers)

	<ul style="list-style-type: none">• Weak Password Protection (Registry settings disallows storage of LANMAN passwords)• Audit Trails Enabled (Allows critical operating system events to be logged)• Microsoft IFC enabled (Allows filtering on ingress ports) <p>Items not in Compliance:</p> <p>x User Accounts (Found multiple, non-password protected user accounts)</p> <p>x Baseline copy of system on secondary storage media (Found on neither primary or secondary)</p> <p>x Open Ports/Default Services (Although Nessus Port Scan results shows 0 holes, there are still 8 open TCP ports; one of which is 445).</p> <p>x File System Integrity (<i>SfcScan</i> DWORDIn registry is not set to 1 which forces the system to scan all protected system files at reboot).</p>																		
Checklist Control 3.1.2 - Checking for Unpatched Systems																			
Objective	To address known issues such as exploited vulnerabilities; faulty code																		
Evidence	▪ Appendix F – MBSA Scan Results																		
Findings	<p>Items in Compliance:</p> <ul style="list-style-type: none">• Microsoft VM Security Updates• Local Account Password Test (No user accounts have simple passwords)• Guest Account (Disabled)• Restrict Anonymous (Computer is properly restricting anonymous access)• IFC (Enabled)• Best Practice – Unnecessary services (No potentially unnecessary services found) <p>Items not in Compliance:</p> <p>Security</p> <p>x (7) Microsoft Office critical updates missing</p> <p>Excel 2002 Security Patch: KB830350 This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>Office XP Security Patch: KB822036 This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>Office XP Service Pack 2 (English version) Office XP Web Services Update: KB812708 This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>Office XP WordPerfect 5.x Converter Security Patch: KB824938 (English version) This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>Outlook 2002 Update: January 22, 2003 This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>Word 2002 Security Patch: KB830346 This update requires Office XP Service Pack 2 (English version) to be installed first.</p> <p>x (5) Microsoft Windows non-critical updates were outdated or unconfirmed</p> <table><thead><tr><th>Security Update</th><th>Description</th><th>Reason</th></tr></thead><tbody><tr><td>Internet Explorer 6</td><td>Internet Explorer 6 Gold</td><td>The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.</td></tr><tr><td>Windows XP Home Edition</td><td>Windows XP Home Edition Gold</td><td>The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.</td></tr><tr><td>MS02-053</td><td>Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)</td><td>Please refer to 306460 for a detailed explanation.</td></tr><tr><td>MS03-030</td><td>Unchecked Buffer in DirectX Could Enable System Compromise (819696)</td><td>Please refer to 306460 for a detailed explanation.</td></tr><tr><td>MS03-051</td><td>Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)</td><td>Please refer to 306460 for a detailed explanation.</td></tr></tbody></table> <p>x (4) Other non-critical updates were outdated (MS02-032, Cumulative Patch for Windows Media Player (Q320920), File version is greater than expected. [C:\WINDOWS\system32\msdxm.ocx, 6.4.9.1128 > 6.4.9.1124]; MDAC 2.7, The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.; MSXML 2.6, The latest service pack for this product is not installed. Currently SP2 is installed. The latest service pack is SP3).</p>	Security Update	Description	Reason	Internet Explorer 6	Internet Explorer 6 Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.	Windows XP Home Edition	Windows XP Home Edition Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.	MS02-053	Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)	Please refer to 306460 for a detailed explanation.	MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.	MS03-051	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Please refer to 306460 for a detailed explanation.
Security Update	Description	Reason																	
Internet Explorer 6	Internet Explorer 6 Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.																	
Windows XP Home Edition	Windows XP Home Edition Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.																	
MS02-053	Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)	Please refer to 306460 for a detailed explanation.																	
MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.																	
MS03-051	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Please refer to 306460 for a detailed explanation.																	

	Windows Non-critical X Automatic Updates (Automatically downloaded, but not automatically installed on this computer) X Administrators (More than 2 found)
	3.1.3 - Checking for Outdated Virus Definitions
Objective	To address having sufficient protection against known issues such as malware
Evidence	<ul style="list-style-type: none"> Appendix E – Current Antivirus Software
Findings	Items in Compliance: <ul style="list-style-type: none"> Antivirus Software (Norton Antivirus 2002)

3.2 – Network/Cable Modem Audit Results

	3.2.1 - Checking for Perimeter Penetration
Objective	To determine if defense-in-depth is needed to eliminate single point of failure
Evidence	<ul style="list-style-type: none"> Appendix C – Nessus Port Scan Results (External) Appendix D – Netstat Port Scan Results (Internal) Appendix G – Microsoft Internet Connection Firewall Appendix H – Sample NeWT Plugins Configurations Appendix I – Sample NeWT Scan Results (SOHO & Windows) Appendix J – Microsoft IFC Configurations
Findings	Items in Compliance: <ul style="list-style-type: none"> 0 vulnerabilities found in all Nessus reports (RPC, Remote File Access, SMTP, SNMP, Useless Services, Windows Users, Firewall) However, there were some informational warnings on services found on certain ports (See Appendix I) Items not in Compliance: None

3.3 – Application Audit Results

	3.3.1 - Checking for Checking for Faulty Installations
Objective	To avoid compromising the system w/default or unknown source installations
Evidence	Appendix E – Add/Remove Programs list (No unlicensed or illegitimate software installed)
Findings	Items in Compliance: <ul style="list-style-type: none"> Automatic check enabled to notify & approve of new installations
	3.3.2 - Checking for Unknown Downloads
Objective	To avoid compromising the system with attachments that contain malware
Evidence	Appendix K – Microsoft Internet Explorer Security Test Results
Findings	Items in Compliance: <ul style="list-style-type: none"> Microsoft Outlook 2002 in use Items not in Compliance: <ul style="list-style-type: none"> Microsoft Internet Explorer CHM File Processing Arbitrary Code Execution Vulnerability -bid9658. (However, there is no patch yet available).

3.3.3 - Checking for Outdated Virus Definitions	
Objective	To avoid compromising the system w/default or unknown source installations
Evidence	Appendix E – Current Antivirus Software
Findings	Items in Compliance: <ul style="list-style-type: none"> • Antivirus Software (Norton Antivirus 2002)
3.3.4 - Checking for Weak Protection of Sensitive Data	
Objective	To avoid improper info disclosure and/or alteration of data
Evidence	Appendix K – Microsoft Internet Explorer Browser Security Test Results
Findings	Items not in Compliance: <ul style="list-style-type: none"> x Microsoft Internet Explorer CHM File Processing Arbitrary Code Execution Vulnerability (bid9658)

3.4 – Operational Audit Results

3.4.1 - Checking for Data Retention Protection	
Objective	To make sure mechanisms are in place to prevent data loss (physically & electronically)
Evidence	No backup mechanisms in place
Findings	Items not in Compliance: <ul style="list-style-type: none"> x Missing Backup mechanisms; Recommended – Zip Drive

3.5 – Physical/Environmental Audit Results

3.5.1 - Checking for Sufficient Fire Detection/Suppression	
Objective	To make sure mechanisms are in place to prevent physical destruction by fire
Evidence	Found working fire extinguisher for acceptable use around computers (First Alert FE1A10G)
Findings	Items in Compliance: <ul style="list-style-type: none"> • UL Rated 1-A:10-B:C (For trash, wood, paper; liquid grease; and electrical fires)

Part 4 –Audit Report

4.1 – Executive Summary

The purpose of this audit report is not to simply present the audit findings, but also explain the company's current compliance position relative to the industry's best practices. This was a relatively small audit undertaking in comparison to larger networked systems and the results were not out of the ordinary. The security posture of this Small Office Home Office is not terribly weak as evidenced by several stimulus/response tests, but there are still a few areas that should be strengthened.

The objective of each component security control was met by the various testing methods and each component did not demonstrate any gaping security holes. If anything, this audit pointed out several shortcomings that need to be addressed with stronger safeguards. Overall, this system is relatively protected against the vulnerabilities outlined in Part 1.

4.2 – Audit Findings

Operating System Results

The operating system in use - Microsoft XP has been known to be a favorite target of attackers due to known vulnerabilities. As a result, the controls were constructed to test default installations; unpatched systems; and outdated virus definitions. The findings were that items in compliance were:

Default Installations

In compliance:

- **Allowable Share Permissions** (No folders or printers)
- **Weak Password Protection** (Registry settings disallows storage of LANMAN passwords)
- **Audit Trails Enabled** (Allows critical operating system events to be logged)
- **Microsoft IFC enabled** (Allows filtering on ingress ports)

Not in compliance:

x User Accounts (Found multiple, non-password protected user accounts)

x Baseline copy of system on secondary storage media (Found on neither primary or secondary)

x Open Ports/Default Services (Although Nessus Port Scan results shows 0 holes, there are still 8 open TCP ports; one of which is 445).

x File System Integrity (*SfcScan* DWORDin registry is not set to 1 which forces the system to scan all protected system files at reboot).

Unpatched Systems

In compliance:

- **Microsoft VM Security Updates**
- **Local Account Password Test** (No user accounts have simple passwords)
- **Guest Account** (Disabled)
- **Restrict Anonymous** (Computer is properly restricting anonymous access)
- **IFC** (Enabled)
- **Best Practice – Unnecessary services** (No potentially unnecessary services found)

Not in compliance:

Security

x (7) Microsoft Office critical updates missing

x (5) Microsoft Windows non-critical updates were outdated or unconfirmed Windows Non-critical

x Automatic Updates (Automatically downloaded, but not automatically installed on this computer)

x Administrators (More than 2 found)

Outdated Virus Definitions

In compliance:

- **Antivirus Software** (Norton Antivirus 2002)

Network/Cable Results

The system is a standalone machine, but connected to the Internet via a Toshiba PCX2500 cable modem – which has been thought to be an insecure network connection method. However, the findings were:

Perimeter Protection

In compliance:

- **0 vulnerabilities found in all Nessus reports. However, there were some informational warnings on services found on certain ports** (See Appendix I)

Application Results

The only item out of compliance was:

x Microsoft Internet Explorer CHM File Processing Arbitrary Code Execution Vulnerability -bid9658. (However, there is no patch yet available).

Operational and Physical Results

Nothing out of compliance.

4.3 – Audit Recommendations

As an IT Security professional, I was surprised at not finding any serious vulnerability in any of this SOHO's components. However, I would recommend installing a third party firewall to catch any external ports that that may have Trojans or spyware on them. Microsoft IFC is a compensating control for systems that rely solely on a personal firewall to block unwanted services and probes.

© SANS Institute 2004, Author retains full rights.

References:

1. COBIT
URL: <http://www.isaca.org/cobit.htm>
2. FISCAM
URL: <http://www.gao.gov/special.pubs/ai12.19.6.pdf>
3. TBS
URL: http://www.tbs-sct.gc.ca/cmo_mfc/Toolkit2/MT_TG/MT01_e.asp
4. The Institute of Internal Auditors
URL: http://www.theiia.org/iaa/index.cfm?doc_id=3061
5. The SANS Top 20 Internet Security Vulnerabilities
URL: <http://www.sans.org/top20/>
6. NTBugtraq.
URL: <http://ntbugtraq.ntadvice.com/default.asp?pid=38&sid=1>
7. "What's new in Security for Windows XP Professional and Windows XP Home Edition".
Microsoft TechNet.
URL: <http://www.microsoft.com/technet/prodtechnol/winxp/evaluate/xpsec.mspx>
8. "Security Basics for Home Users". Microsoft Security.
URL: <http://www.microsoft.com/security/home/>
9. "Default settings for services". Microsoft Windows XP Home.
URL: http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=WINDOWSXP/home/using/productdoc/en/sys_srv_default_settings.asp
10. "List of Services Needed to run a Secure IIS Computer". Microsoft Knowledge Base Article - 189271.
URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;189271>
11. "Description of Windows XP & Windows Server 2003 System File Checker". Microsoft Knowledge Base Article -310747.
URL: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;310747>
12. Bradley, Tony. "Win2k Boot Disc Can Bypass Windows XP Passwords". Windows XP Security "Flaw". Internet/Network Security. About.com
URL: <http://netsecurity.about.com/library/weekly/aa021603a.htm>
13. Bradley, Tony. "Security Basics At Home". Internet/Network Security. About.com
URL: <http://netsecurity.about.com/library/weekly/aa011003a.htm>
14. Questions and Answers: Security 1.2. The Cable Modem Reference Guide. Cable-Modems.org.
URL: <http://www.cable-modems.org/q&a/#1.2>

15. "How big an issue is security for the Internet, broadband and my computer?". Getting Connected: Security. Cable-Modems.net.
URL: <http://www.cable-modem.net/gc/security.html>
16. Stewart, M. James. "Facing the security risks of cable modems".
8 July, 2002. ZDNet UK.
URL: <http://insight.zdnet.co.uk/hardware/servers/0,39020445,2118716,00.htm>
17. "Security in DOCSIS-based Cable Modem systems". Section 2: Security of Data Transport Services. Page 2.
URL: http://www.cablemodem.com/downloads/Security_in_DOCSIS.pdf
18. McKelvey, T. Joel. Cisco Systems, Inc., USA. "Combating security risks on the cable IP network". IBC 2002 Conference Papers.
URL: <http://www.broadcastpapers.com/broadband/IBCCiscoSecurityCableIP01.htm>
19. Microsoft Windows XP Security Guide Overview. Microsoft TechNet.
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/winclnt/secwinxp/default.asp>
20. "5- Minute Security Advisor: Essential Security Tools for Home Office and Power Users". Hardening Systems and Servers: Checklists and Guides. Microsoft TechNet.
URL: <http://www.microsoft.com/technet/security/topics/hardsys/default.msp>
21. Weigel, Ray. "Windows XP comes packed with a down and dirty firewall". Inside XP: Internet Connection Firewall. Products and Reviews. 30 September, 2001. Techtv.
URL: <http://www.techtv.com/products/software/story/0,23008,3338448,00.html>
22. "How to manually open ports in the Windows XP Internet Connection Firewall". Protect your PC. 7 November, 2003. Microsoft Security.
URL: <http://www.microsoft.com/security/protect/ports.asp>
23. Wolfblade. "Windows XP Internet Connection Firewall. GameSpy Arcade [HELP]ers
URL: <http://www.gamespyarcade.com/helpers/workshop/xpfirewall/>
24. Meier, D. J. Mackman, Alex. Dunner, Michael. Vasireddy, Srinath. Escamilla, Ray. Murukan, Anandha. "Checklist: Securing Data Access". Improving Web Application Security: Threats and Countermeasures. June 2003. Microsoft TechNet.
URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnsec/html/CL_SecuDat.asp
25. "Understanding the Security Risk Management Discipline". Security Policy, Assessment, and Vulnerability Analysis. Microsoft TechNet.
URL: <http://www.microsoft.com/technet/security/topics/assess/default.msp>
26. McCarthy, Kieren. "New Explorer hole could be devastating". 28 January, 2004
Techworld.com.
URL: http://www.infoworld.com/article/04/01/28/HNehole_1.html
27. OWASP (The Open Web Application Security Project)
URL: <http://www.owasp.org/index>
28. "Understand and maintain security with Internet Explorer". Microsoft Internet Explorer Home. 22 October 2003.
URL: <http://www.microsoft.com/windows/ie/security/default.asp>
29. "Which versions of Internet Explorer are Affected by Security Issues?". Internet Explorer Security Issues. Microsoft Internet Explorer Security Center.
URL: <http://www.nwnetworks.com/iesecurity.htm>
30. Internet Explorer security – Georgi Guninski Security Research
URL: <http://www.guninski.com/browsers.html>
31. Doemberg, Curt. "Guide to Securing Microsoft Internet Explorer 5.5 Security Using Group Policy". National Security Agency Security Recommendation Guides. Version 1.0. July 2002.
URL: <http://nsa2.www.conxion.com/support/guides/sd-8.pdf>
32. "Using Office Security features". 9 March, 2004. Microsoft Security
URL: <http://www.microsoft.com/security/articles/officesec.asp>
33. Seltzer, Larry. "Fresh Worms Attack E-mail, Internet Explorer, User Data". 25 February 2004. eWeek Enterprise News & Reviews.
URL: <http://www.eweek.com/article2/0,1759,1538954,00.asp>

34. Outlook Email Security Update. 19 February 2004. Slipstick Systems.
URL: <http://www.slipstick.com/outlook/esecup.htm>
35. "Help protect your Inbox from email viruses". Security features for Outlook 2002 and previous versions. 26 April, 2002. Microsoft Office Online.
URL: <http://www.microsoft.com/office/previous/outlook/2002security.asp>

Appendix A

XP system baseline (excerpt of file)

System Information report written at: 3/4/2004 12:42:46 PM

System Name: USER

[System Summary]

Item Value

OS Name Microsoft Windows XP Home Edition

Version 5.1.2600 Build 2600

OS Manufacturer Microsoft Corporation

System Name USER

System Manufacturer Dell Computer Corporation

System Model Dimension 8250

System Type X86-based PC

Processor x86 Family 15 Model 2 Stepping 7 GenuineIntel ~2651 Mhz

BIOS Version/Date Dell Computer Corporation A00, 10/4/2002

SMBIOS Version 2.3

Windows Directory C:\WINDOWS

System Directory C:\WINDOWS\System32

Boot Device \Device\HarddiskVolume2

Locale United States

Hardware Abstraction Layer Version = "5.1.2600.0 (xpclient.010817-1148)"

User Name USER\XYZ COMPANY

Time Zone Eastern Standard Time

Total Physical Memory 256.00 MB

Available Physical Memory 32.67 MB

Total Virtual Memory 880.23 MB

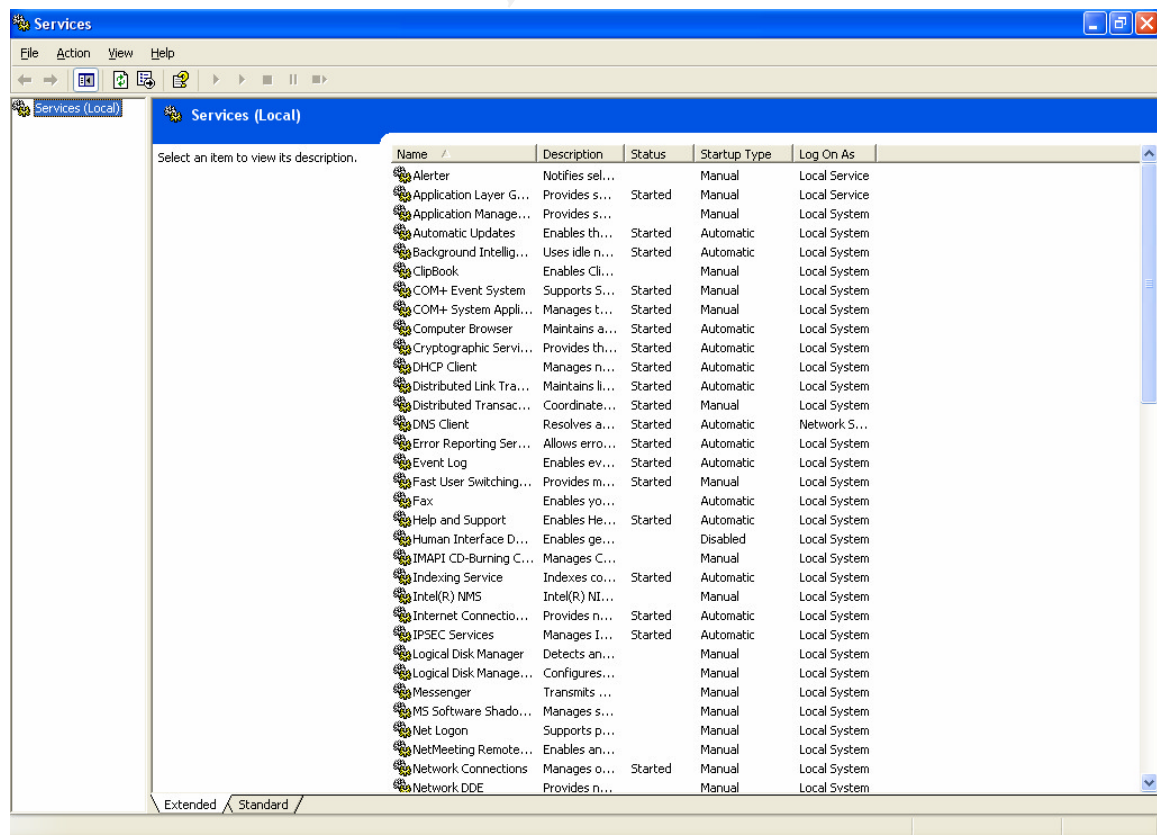
Available Virtual Memory 210.57 MB

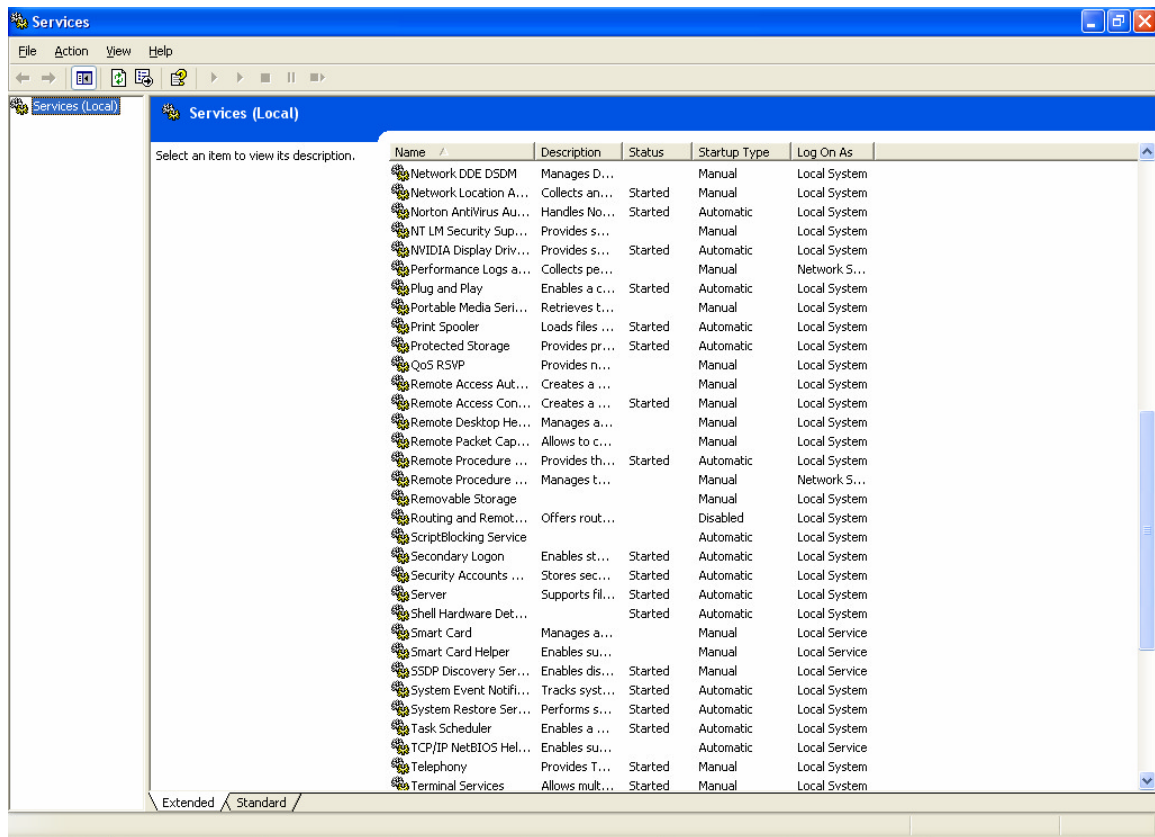
Page File Space 625.25 MB

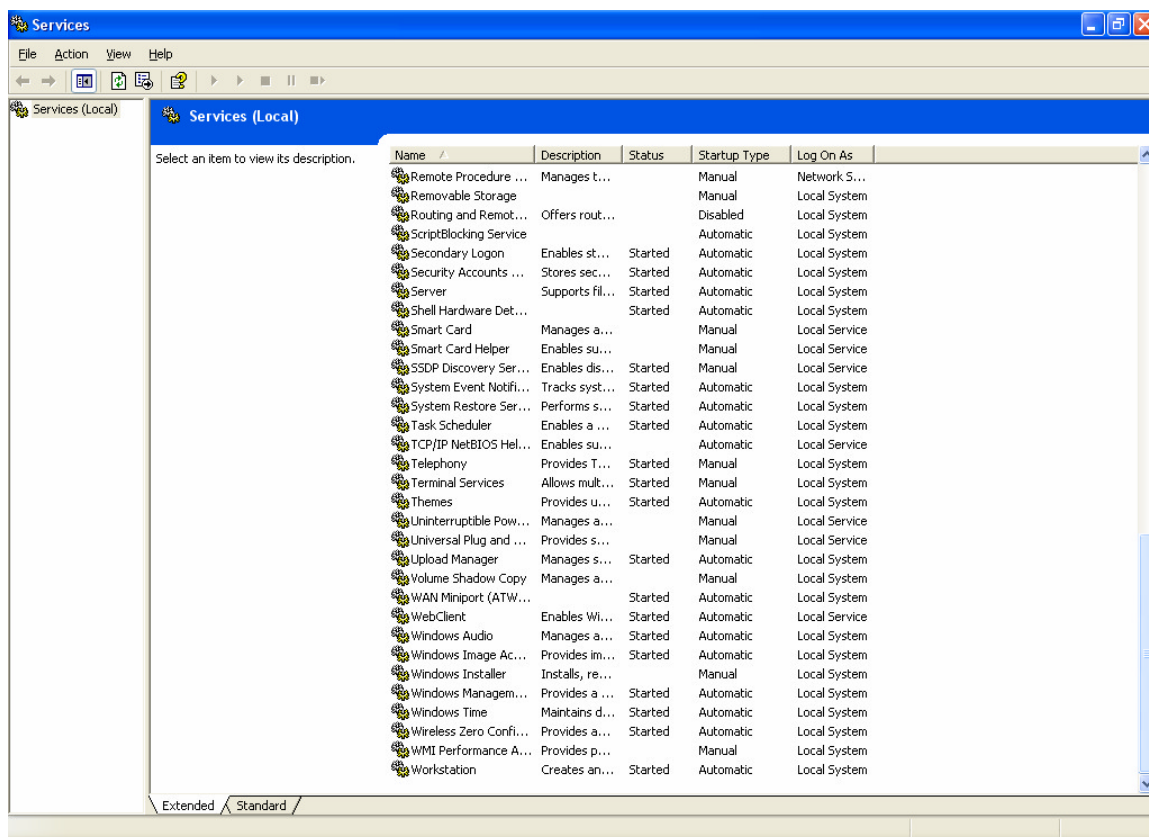
Page File C:\pagefile.sys

Appendix B

Snapshot of Local Services Running







Appendix C

Nessus Port Scan Results (External)

Start Time: Mon Mar 15 14:15:46 2004 Tenable NeWT Security Reports Finish Time: Mon Mar 15 14:18:55 2004

xxx.xxx.xxx.xxx




xxx.xxx.xxx.xxx

8 Open Ports, 8 Notes, 0 Infos, 0 Holes.


xxx.xxx.xxx.xxx

[\[Return to top\]](#)


epmap (135/tcp)

 Port is open
Plugin ID : [11219](#)


microsoft-ds (445/tcp)

 Port is open
Plugin ID : [11219](#)


unknown (1024/tcp)

 Port is open
Plugin ID : [11219](#)

blackjack (1025/tcp)

 Port is open
Plugin ID : [11219](#)


activesync (1034/tcp)

 Port is open
Plugin ID : [11219](#)


unknown (1044/tcp)

 Port is open
Plugin ID : [11219](#)

vipremoteagent (3752/tcp)

 Port is open
Plugin ID : [11219](#)

complex-main (5000/tcp)

 Port is open
Plugin ID : [11219](#)

Appendix D

Netstat Port Scan Results (Internal)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\XYZcompany >netstat -na

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3038	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3042	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3540	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING
TCP	24.215.134.94:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1241	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1242	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3008	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3291	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3536	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3539	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3539	127.0.0.1:3540	ESTABLISHED
TCP	127.0.0.1:3540	127.0.0.1:3539	ESTABLISHED
TCP	127.0.0.1:5180	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:3004	*.*	
UDP	0.0.0.0:3032	*.*	
UDP	0.0.0.0:3124	*.*	
UDP	x.x.x.x:123	*.*	
UDP	x.x.x.x:137	*.*	
UDP	x.x.x.x:138	*.*	
UDP	x.x.x.x:1900	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1900	*.*	
UDP	127.0.0.1:3009	*.*	
UDP	127.0.0.1:3012	*.*	
UDP	127.0.0.1:3292	*.*	
UDP	127.0.0.1:3313	*.*	
UDP	127.0.0.1:3399	*.*	
UDP	127.0.0.1:3537	*.*	
UDP	127.0.0.1:3541	*.*	
UDP	127.0.0.1:4217	*.*	
UDP	127.0.0.1:4523	*.*	
UDP	127.0.0.1:4595	*.*	
UDP	127.0.0.1:4727	*.*	

C:\Documents and Settings\XYZcompany >netstat -o

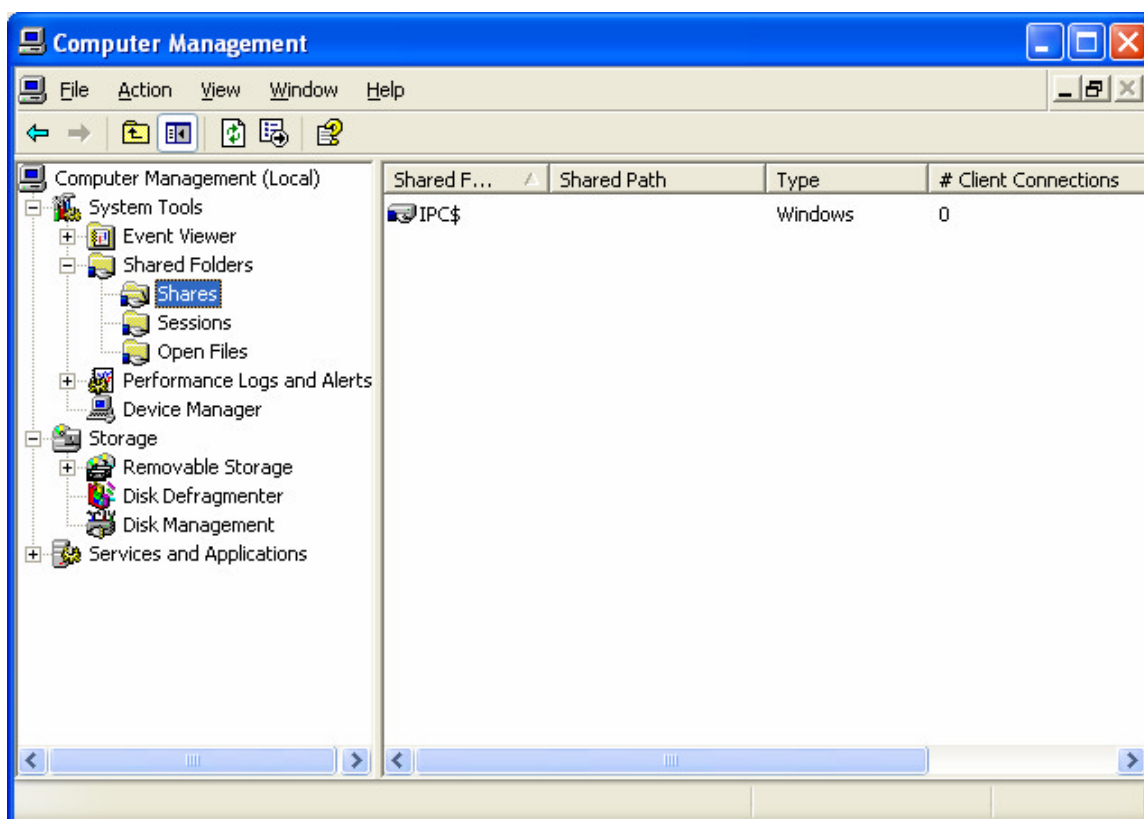
Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	company:3539	localhost:3540	ESTABLISHED	3732
TCP	company:3540	localhost:3539	ESTABLISHED	3732

C:\Documents and Settings\XYZcompany>

Appendix E

Allowable Share Permissions



© SANS Institute 2004

Appendix F

MBSA Scan Results

Computer name: MSHOME\XYZ COMPANY
IP address: x.x.x.x
Security report name: MSHOME – XYZ COMPANY (3-9-2004 12:30 AM)
Scan date: 3/9/2004 12:30 AM
Security update database version: 2004.02.10.0
Office update database version: 11.0.0.6206
Security assessment: Potential Risk (One or more non-critical checks failed.)

Security Updates

Score	Issue	Result																		
Check failed (critical)	Office Security Updates	7 security updates are missing. Update Excel 2002 Security Patch: KB830350 This update requires Office XP Service Pack 2 (English version) to be installed first. Office XP Security Patch: KB822036 This update requires Office XP Service Pack 2 (English version) to be installed first. Office XP Service Pack 2 (English version) Office XP Web Services Update: KB812708 This update requires Office XP Service Pack 2 (English version) to be installed first. Office XP WordPerfect 5.x Converter Security Patch: KB824938 (English version) This update requires Office XP Service Pack 2 (English version) to be installed first. Outlook 2002 Update: January 22, 2003 This update requires Office XP Service Pack 2 (English version) to be installed first. Word 2002 Security Patch: KB830346 This update requires Office XP Service Pack 2 (English version) to be installed first.																		
Check failed (non-critical)	Windows Security Updates	5 security updates are out of date or could not be confirmed. <table><tr><th>Security Update</th><th>Description</th><th>Reason</th></tr><tr><td>Internet Explorer 6</td><td>Internet Explorer 6 Gold</td><td>The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.</td></tr><tr><td>Windows XP Home Edition</td><td>Windows XP Home Edition Gold</td><td>The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.</td></tr><tr><td>MS02-053</td><td>Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)</td><td>Please refer to 306460 for a detailed explanation.</td></tr><tr><td>MS03-030</td><td>Unchecked Buffer in DirectX Could Enable System Compromise (819696)</td><td>Please refer to 306460 for a detailed explanation.</td></tr><tr><td>MS03-051</td><td>Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)</td><td>Please refer to 306460 for a detailed explanation.</td></tr></table>	Security Update	Description	Reason	Internet Explorer 6	Internet Explorer 6 Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.	Windows XP Home Edition	Windows XP Home Edition Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.	MS02-053	Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)	Please refer to 306460 for a detailed explanation.	MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.	MS03-051	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Please refer to 306460 for a detailed explanation.
Security Update	Description	Reason																		
Internet Explorer 6	Internet Explorer 6 Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.																		
Windows XP Home Edition	Windows XP Home Edition Gold	The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.																		
MS02-053	Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)	Please refer to 306460 for a detailed explanation.																		
MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.																		
MS03-051	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Please refer to 306460 for a detailed explanation.																		
Check failed (non-critical)	Windows Media Player Security Updates	1 security updates are out-of-date. <table><tr><th>Security Update</th><th>Description</th><th>Reason</th></tr><tr><td>MS02-032</td><td>Cumulative Patch for</td><td>File version is greater than expected. [C:\WINDOWS\system32\msdxm.ocx,</td></tr></table>	Security Update	Description	Reason	MS02-032	Cumulative Patch for	File version is greater than expected. [C:\WINDOWS\system32\msdxm.ocx,												
Security Update	Description	Reason																		
MS02-032	Cumulative Patch for	File version is greater than expected. [C:\WINDOWS\system32\msdxm.ocx,																		

	Windows Media Player (Q320920)	6.4.9.1128 > 6.4.9.1124]	
Check failed (non-critical)	MDAC Security Updates	1 security updates are out-of-date.	
	Security Update MDAC 2.7	Description MDAC 2.7 Gold	Reason The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP1.
Check failed (non-critical)	MSXML Security Updates	2 security updates are out-of-date.	
	Security Update MSXML 2.6	Description MSXML 2.6 SP2	Reason The latest service pack for this product is not installed. Currently SP2 is installed. The latest service pack is SP3.
	MSXML 3.0	MSXML 3.0 SP2	The latest service pack for this product is not installed. Currently SP2 is installed. The latest service pack is SP4.
Check passed	Microsoft VM Security Updates	No critical security updates are missing.	

Windows Scan Results

Vulnerabilities

Score	Issue	Result																																								
Check failed (non-critical)	Automatic Updates	Updates are automatically downloaded, but not automatically installed on this computer.																																								
Check failed (non-critical)	Administrators	More than 2 Administrators were found on this computer. <div>User Administrator XYZ COMPANY S-1-5-21-240772092-4217759621-2681017343-1003</div>																																								
Check passed	Local Account Password Test	No user accounts have simple passwords. <table><tr><th>User</th><th>Weak Password</th><th>Locked Out</th><th>Disabled</th></tr><tr><td>Guest</td><td>-</td><td>-</td><td>Disabled</td></tr><tr><td>SUPPORT_388945a0</td><td>-</td><td>-</td><td>Disabled</td></tr><tr><td>SUPPORT_3f151ab9</td><td>-</td><td>-</td><td>Disabled</td></tr><tr><td>Administrator</td><td>-</td><td>-</td><td>-</td></tr><tr><td>HelpAssistant</td><td>-</td><td>-</td><td>-</td></tr><tr><td>MG1</td><td>-</td><td>-</td><td>-</td></tr><tr><td>MG2</td><td>-</td><td>-</td><td>-</td></tr><tr><td>USER</td><td>-</td><td>-</td><td>-</td></tr><tr><td>SG1</td><td>-</td><td>-</td><td>-</td></tr></table>	User	Weak Password	Locked Out	Disabled	Guest	-	-	Disabled	SUPPORT_388945a0	-	-	Disabled	SUPPORT_3f151ab9	-	-	Disabled	Administrator	-	-	-	HelpAssistant	-	-	-	MG1	-	-	-	MG2	-	-	-	USER	-	-	-	SG1	-	-	-
User	Weak Password	Locked Out	Disabled																																							
Guest	-	-	Disabled																																							
SUPPORT_388945a0	-	-	Disabled																																							
SUPPORT_3f151ab9	-	-	Disabled																																							
Administrator	-	-	-																																							
HelpAssistant	-	-	-																																							
MG1	-	-	-																																							
MG2	-	-	-																																							
USER	-	-	-																																							
SG1	-	-	-																																							
Check passed	File System	All hard drives (1) are using the NTFS file system. <table><tr><th>Drive Letter</th><th>File System</th></tr><tr><td>C:</td><td>NTFS</td></tr></table>	Drive Letter	File System	C:	NTFS																																				
Drive Letter	File System																																									
C:	NTFS																																									
Check passed	Guest Account	The Guest account is disabled on this computer.																																								
Check passed	Restrict Anonymous	Computer is properly restricting anonymous access.																																								
Check passed	Internet Connection Firewall	Internet Connection Firewall is enabled on all network connections. <table><tr><th>Connection Name</th><th>Firewall</th><th>Open Ports</th></tr><tr><td>1394 Connection</td><td>Enabled</td><td>-</td></tr><tr><td>EARTHLINK</td><td>Enabled</td><td>-</td></tr><tr><td>Local Area Connection</td><td>Enabled</td><td>-</td></tr></table>	Connection Name	Firewall	Open Ports	1394 Connection	Enabled	-	EARTHLINK	Enabled	-	Local Area Connection	Enabled	-																												
Connection Name	Firewall	Open Ports																																								
1394 Connection	Enabled	-																																								
EARTHLINK	Enabled	-																																								
Local Area Connection	Enabled	-																																								
Check not performed	Autologon	Check is skipped on Windows XP Home Edition computers.																																								
Check not performed	Password Expiration	Check is skipped on Windows XP Home Edition computers.																																								

Additional System Information

Score	Issue	Result
Best practice	Auditing	Check is skipped on Windows XP Home Edition computers.
Best practice	Services	No potentially unnecessary services were found.

Additional information	Shares	No shares are present on your computer.
Additional information	Windows Version	Computer is running Windows 2000 or greater.

SQL Server Scan Results

Score	Issue	Result
Check not performed	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

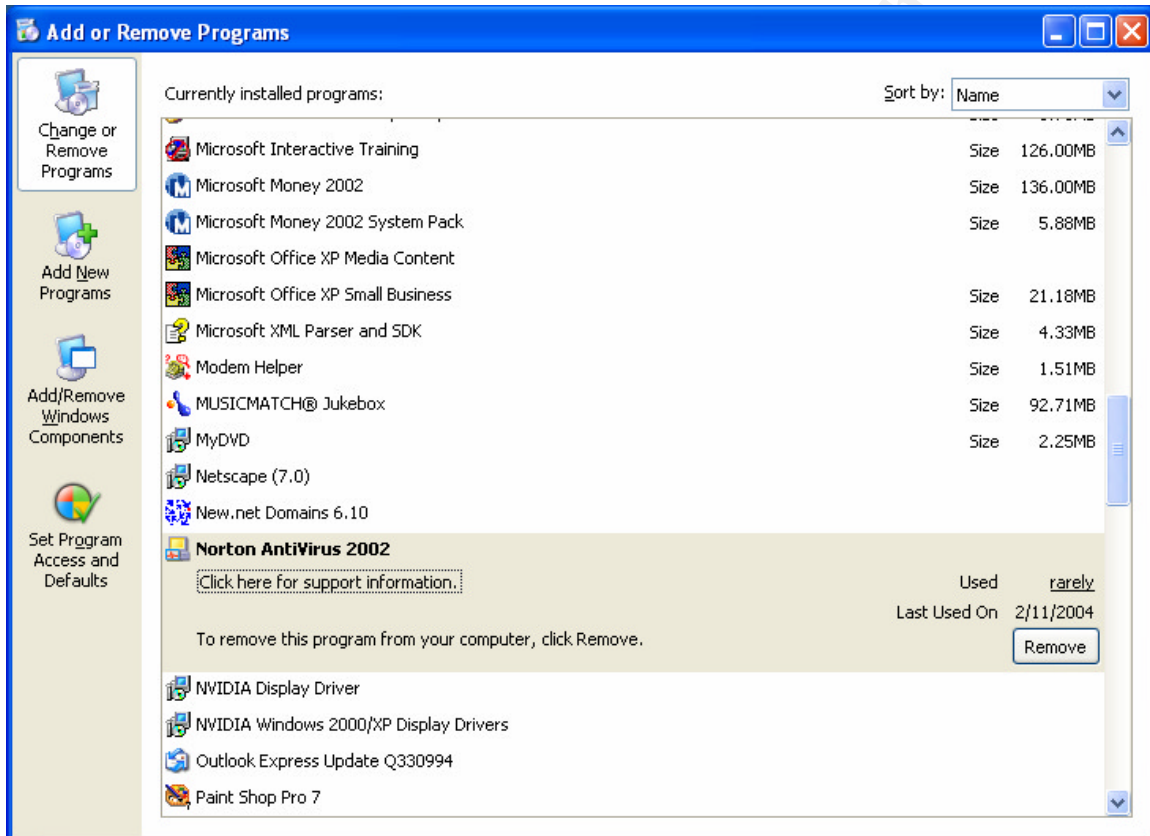
Vulnerabilities

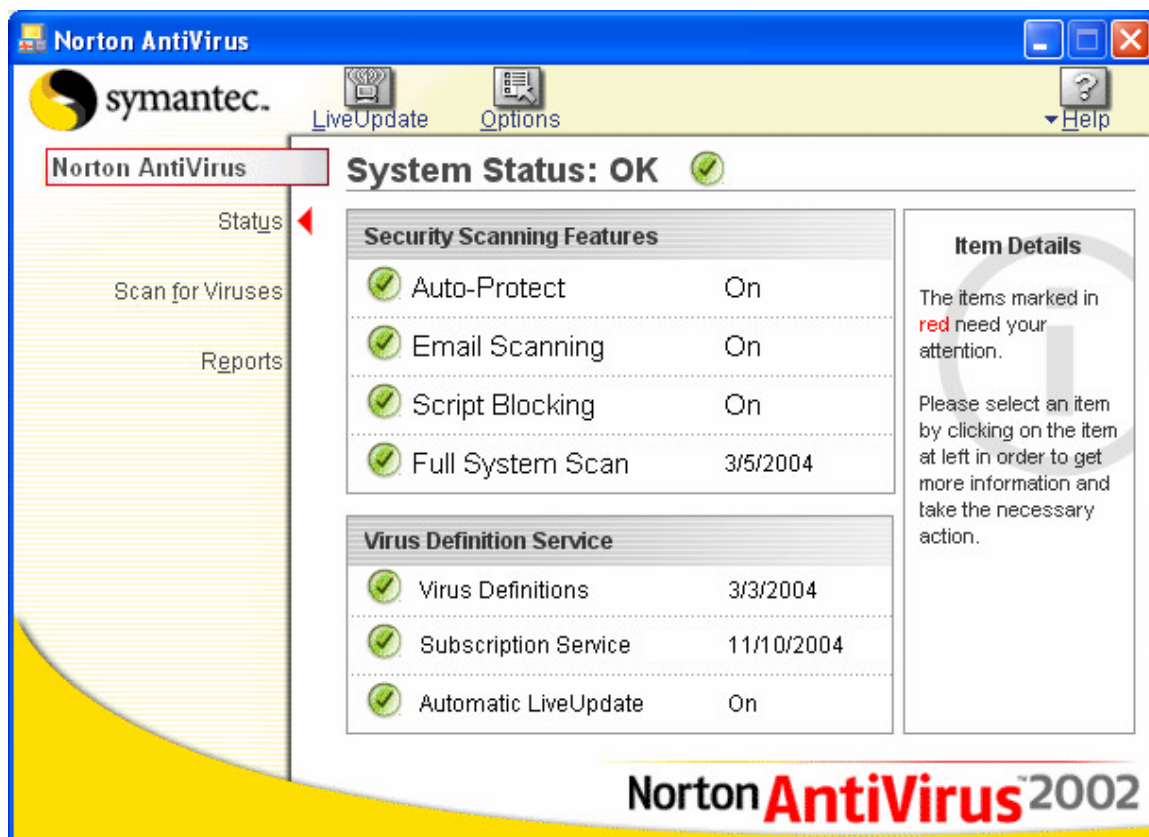
Score	Issue	Result
Check passed	IE Zones	Internet Explorer zones have secure settings for all users.
Check passed	Macro Security	3 Microsoft Office product(s) are installed. No issues were found.
	Issue	User
	Microsoft Excel 2002	All Users
	Microsoft Outlook 2002	All Users
	Microsoft Word 2002	All Users
		Advice
		No security issues were found.
		No security issues were found.
		No security issues were found.

© SANS Institute 2004, Author retains all rights.

Appendix G

Current Antivirus Software



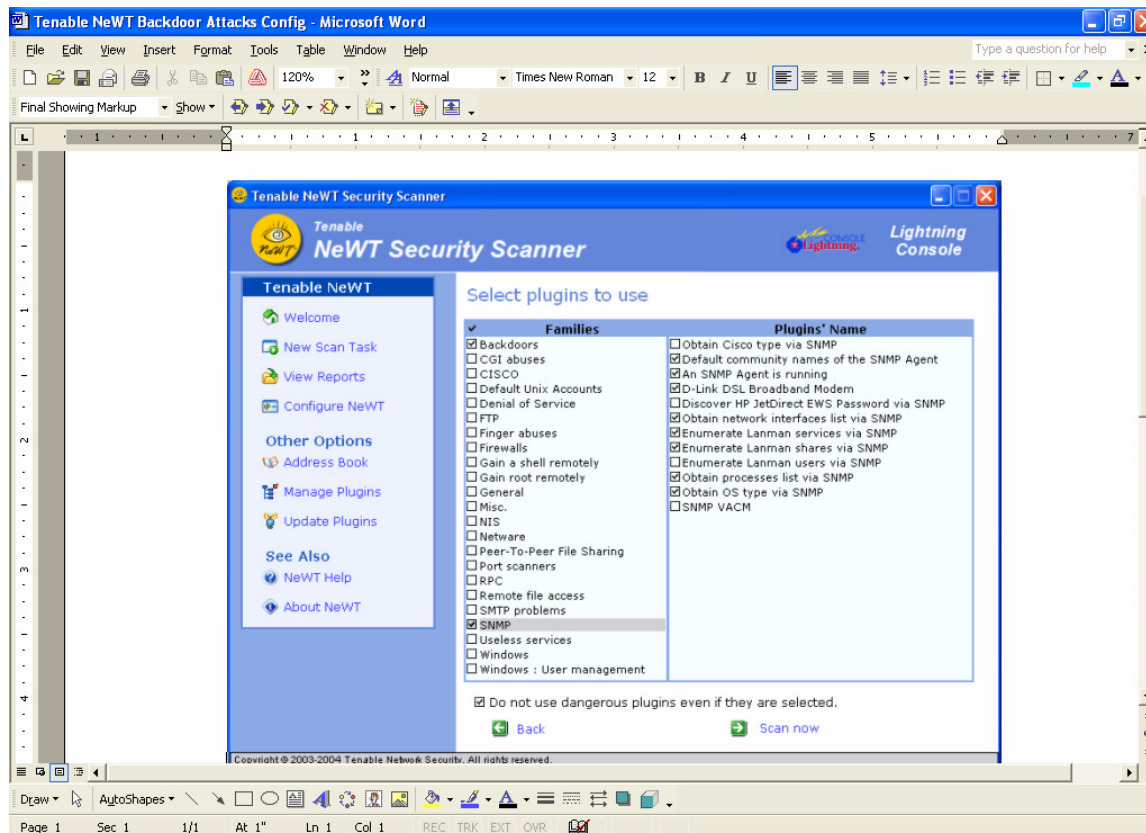


© SANS Institute 2004, A

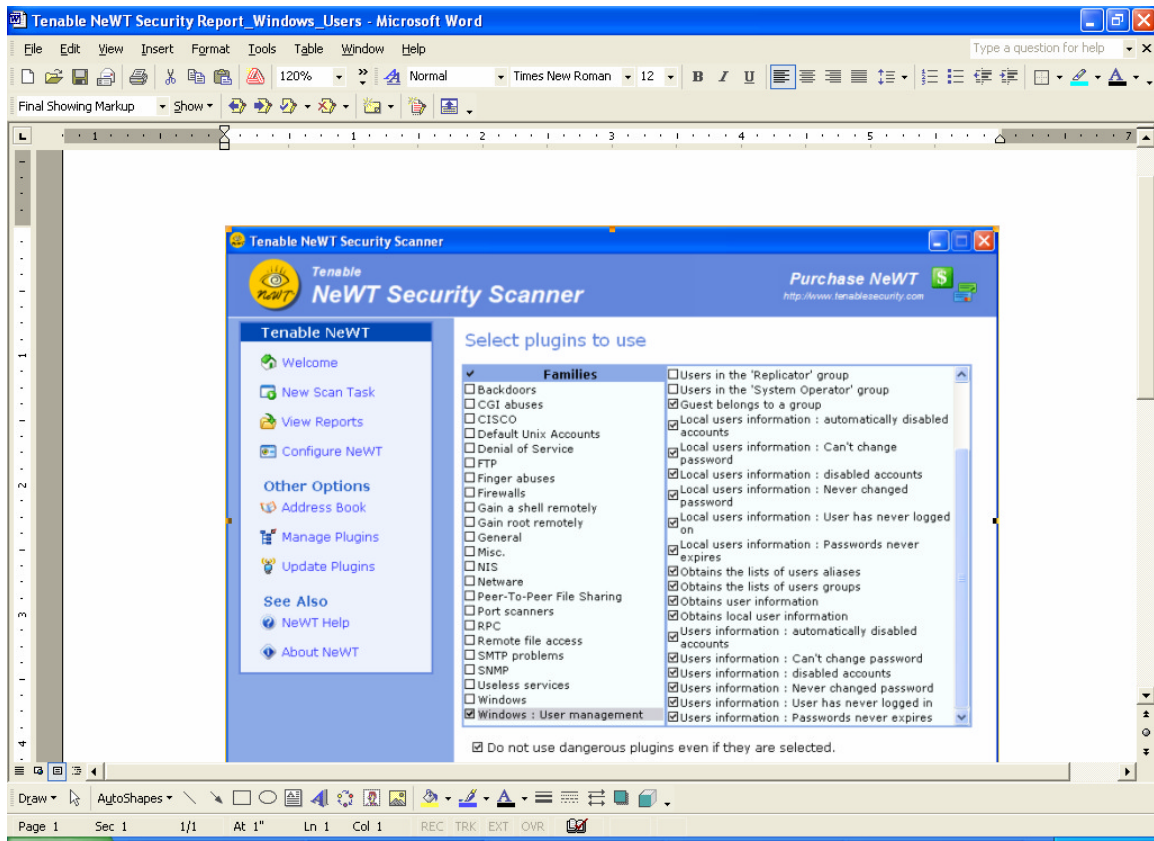
Appendix H

Sample NeWT Plugins Configurations

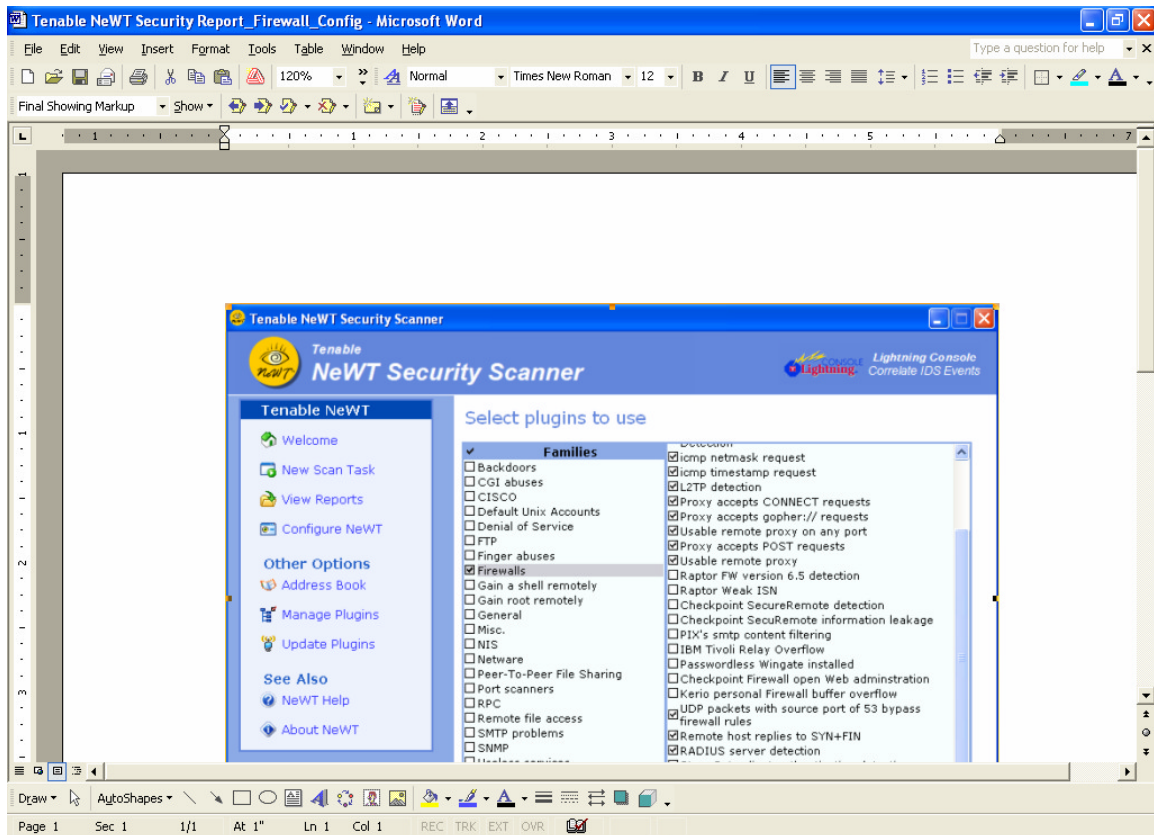
Backdoor



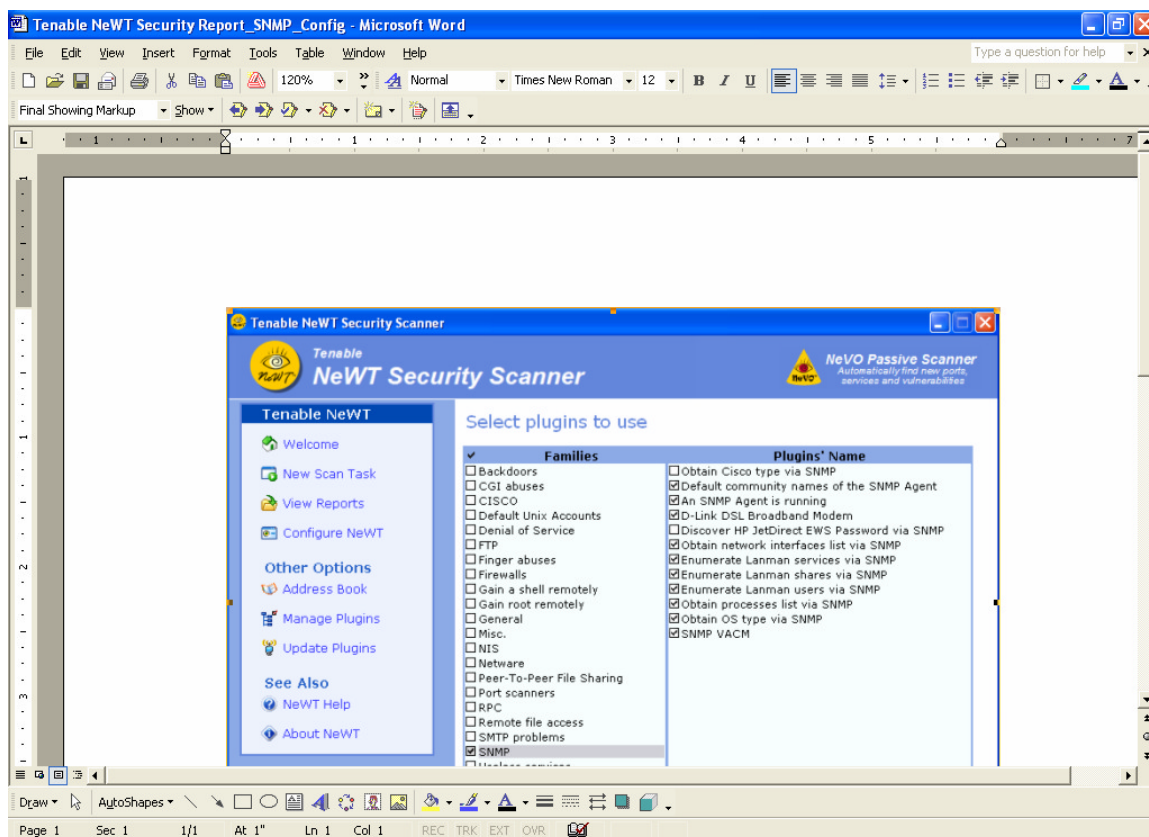
Windows Users



Firewalls

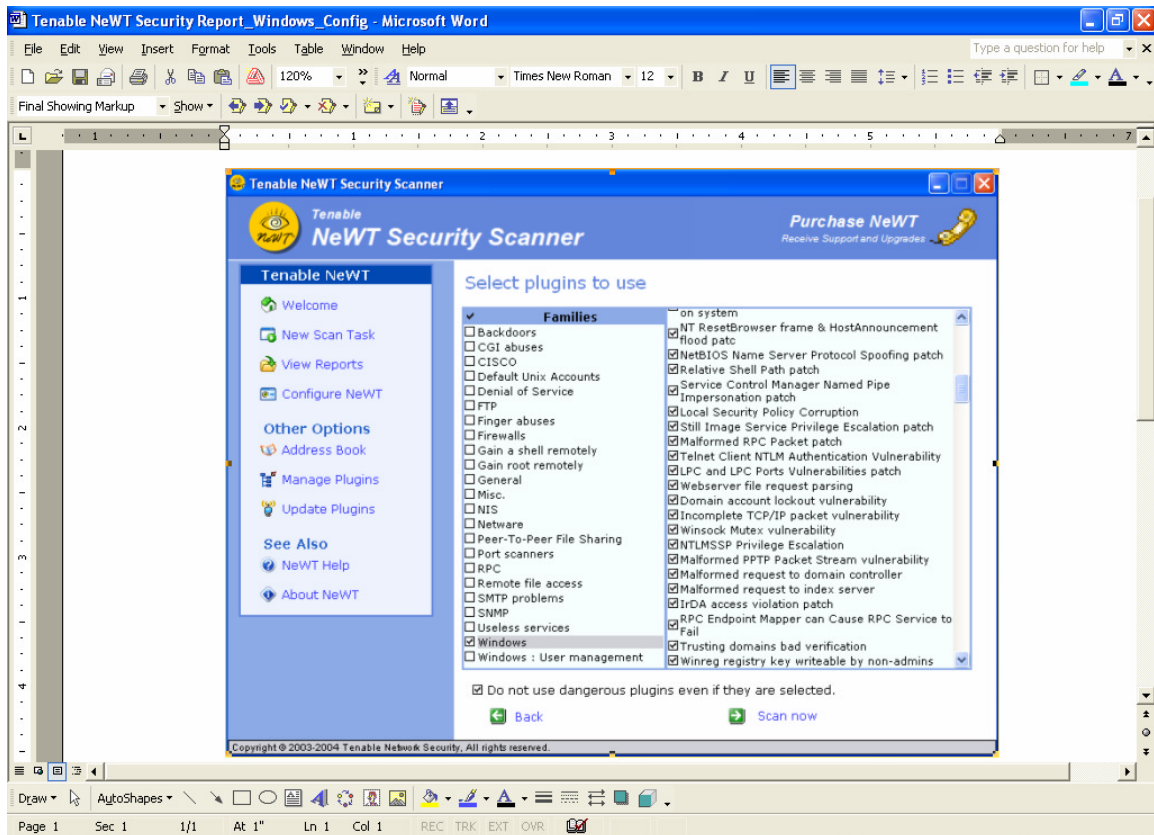


SNMP



Windows

© SANS Institute 2004, All Rights Reserved.



Appendix I

Sample NeWT Scan Results

SOHO Scan Results

Tenable NeWT Security Reports

Start Time: Mon Mar 15 14:21:49 2004

Finish Time: Mon Mar 15 14:25:29 2004

localhost



[x.x.x.x](#)

8 Open Ports, 13 Notes, 3 Infos, 0 Holes.

127.0.0.1

[\[Return to top\]](#)



Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

epmap (135/tcp)

Solution : filter incoming traffic to this port.
Risk factor : Low

Plugin ID : [10736](#)



Port is open
Plugin ID : [11219](#)



The host Security Identifier (SID) can be obtained remotely. Its value is :

USER : 5-21-240772092--77207675--1613949953

An attacker can use it to obtain the list of the local users of this host

Solution : filter the ports 137-139 and 445
Risk factor : Low

CVE : CVE-2000-1200
BID : 959

microsoft-ds (445/tcp)

Plugin ID : [10859](#)



Port is open
Plugin ID : [11219](#)



A CIFS server is running on this port
Plugin ID : [11011](#)



It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).

Note that this won't completely disable null sessions, but will prevent them from connecting to IPC\$

Please see <http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html>

All the smb tests will be done as "/"

CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117

BID : 494, 990

Plugin ID : [10394](#)



Port is open
Plugin ID : [11219](#)



An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
Jade
Latinus
NetSpy
Remote Administration Tool - RAT [no 2]

unknown (1024/tcp)

Unless you know for sure what is behind it, you'd better check your system

Anyway, don't panic, Nessus only found an open port. It may have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner

Risk factor : Low

Plugin ID : [11157](#)



Port is open
Plugin ID : [11219](#)



Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

blackjack (1025/tcp)

Here is the list of DCE services running on this port:

UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:x.x.x[1025]

UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:x.x.x[1025]


UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
Endpoint: ncacn_ip_tcp:x.x.x[1025]


Solution : filter incoming traffic to this port.
Risk Factor : Low

Plugin ID : [10736](#)

activesync (1034/tcp)  Port is open
Plugin ID : [11219](#)

unknown (1044/tcp)  Port is open
Plugin ID : [11219](#)

 Port is open
Plugin ID : [11219](#)

 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

vipremoteagent (3752/tcp)

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]


UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

Solution : filter incoming traffic to this port.
Risk Factor : Low

Plugin ID : [10736](#)

complex-main (5000/tcp)  The remote host is running Microsoft UPnP TCP helper.


If the tested network is not a home network, you should disable this service.

Solution : Set the following registry key :
Location : HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV

Key : Start
Value : 0x04

Risk Factor : Low
CVE : CVE-2001-0876
BID : 3723

Plugin ID : [11765](#)

 Port is open
Plugin ID : [11219](#)

Windows Scan Results

Tenable NeWT Security Reports

Start Time: Mon Mar 15 16:27:59 2004 Finish Time: Mon Mar 15 16:28:08 2004

localhost



[x.x.x.x](#)

5 Open Ports, 4 Notes, 3 Infos, 0 Holes.

x.x.x.x

[\[Return to top\]](#)



The remote host is running Microsoft UPnP TCP helper.

If the tested network is not a home network, you should disable this service.

Solution : Set the following registry key :

Location : HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV

Key : Start

Value : 0x04

complex-main
(5000/tcp)

Risk Factor : Low
CVE : CVE-2001-0876
BID : 3723

Plugin ID : [11765](#)



The host Security Identifier (SID) can be obtained remotely. Its value is :

USER : 5-21-240772092--77207675--1613949953

microsoft-ds (445/tcp)


An attacker can use it to obtain the list of the local users of this host


Solution : filter the ports 137-139 and 445

Risk factor : Low

CVE : CVE-2000-1200
BID : 959


Plugin ID : [10859](#)

 A CIFS server is running on this port
Plugin ID : [11011](#)

 It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).
Note that this won't completely disable null sessions, but will prevent them from connecting to IPC\$
Please see <http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html>

All the smb tests will be done as "/"
CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117
BID : 494, 990
Plugin ID : [10394](#)


 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

epmap (135/tcp)

Solution : filter incoming traffic to this port.
Risk factor : Low

Plugin ID : [10736](#)

 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

blackjack (1025/tcp)

UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[1025]


UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[1025]

UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[1025]

Solution : filter incoming traffic to this port.

Risk Factor : Low

Plugin ID : [10736](#)

 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

vipremoteagent
(3752/tcp)

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:x.x.x.x[3752]

Solution : filter incoming traffic to this port.

Risk Factor : Low

Plugin ID : [10736](#)

SNMP Scan Results (Same for RPC, Remote file access, SMTP, Useless Services, Windows Users, Firewall)

Tenable NeWT Security Reports

Start Time: Mon Mar 15 16:33:48 2004

Finish Time: Mon Mar 15 16:33:53 2004

x.x.x.x

No Vulnerability Found.

Appendix K

Microsoft Internet Explorer Browser Security Test Results

Browser Security Test Results

Dear Customer,

The Browser Security Test is finished. Please find the results below:

High Risk Vulnerabilities 1
Medium Risk Vulnerabilities 0
Low Risk Vulnerabilities 0

New bugs keep coming! [Sign up for announcements of new tests.](#)

Questions about the test? [Read the FAQ.](#)

Still having questions? Send us [your feedback.](#)

Want to know how everyone else is doing on Browser Test? Check [our statistics.](#)

High Risk Vulnerabilities

Microsoft Internet Explorer CHM File Processing Arbitrary Code Execution Vulnerability (bid9658)

Description

This bug can allow a malicious web site to automatically download and execute programs on your computer without your knowledge. This means that an attacker could infect your computer with a virus or install a program which may allow them to take control of your computer.

There is a virus found in the wild that uses this bug to infect computers.

Technical Details

CHM files are "Compiled HTML Help" files. This is a proprietary Microsoft format used for storing help files in Windows applications. CHM files can contain multiple HTML pages, tables of contents, indexes, etc.

When a CHM file is opened from a local disk, it is treated as trusted content, and the execution of scripts in CHM file is not restricted in any way. They can therefore start programs, write data to the disk, and so on.

When a user attempts to open a CHM file from a remote web site, normally Internet Explorer displays a dialog box asking what to do with the file. The dialog box includes a warning saying that the file can contain malicious content and allows the user to save the file without opening it.

This bug allows to bypass the warning from Internet Explorer and download and run a CHM file automatically. This is done by redirecting the IFRAME to a specially crafted URL like this: "URL:ms-its: mhtml:file://C:\ss.MHT!http://www.example.com//chm.chm::files/launch.htm" Internet Explorer will download chm.chm file from the specified website and execute it without warning the user. The CHM file can contain scripts that will have complete access to the user's computer.

Recommendations

No patch is available for this problem yet. A possible workaround is to disable Active Scripting in Internet Explorer "Local Computer" zone.

Follow these steps to disable Active Scripting in "Local Computer" zone. **Warning: This procedure requires editing the registry. If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.**

1. Start Registry Editor (Click "Start" button, choose "Run", type "regedit" and click OK).
2. Locate the following key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only and set it to the value of 1
3. Locate the following key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1400 and set it to the value of 3
4. Restart Internet Explorer
5. For more information about restricting the "Local Computer" zone see [Microsoft Knowledge Base article 182569](#)

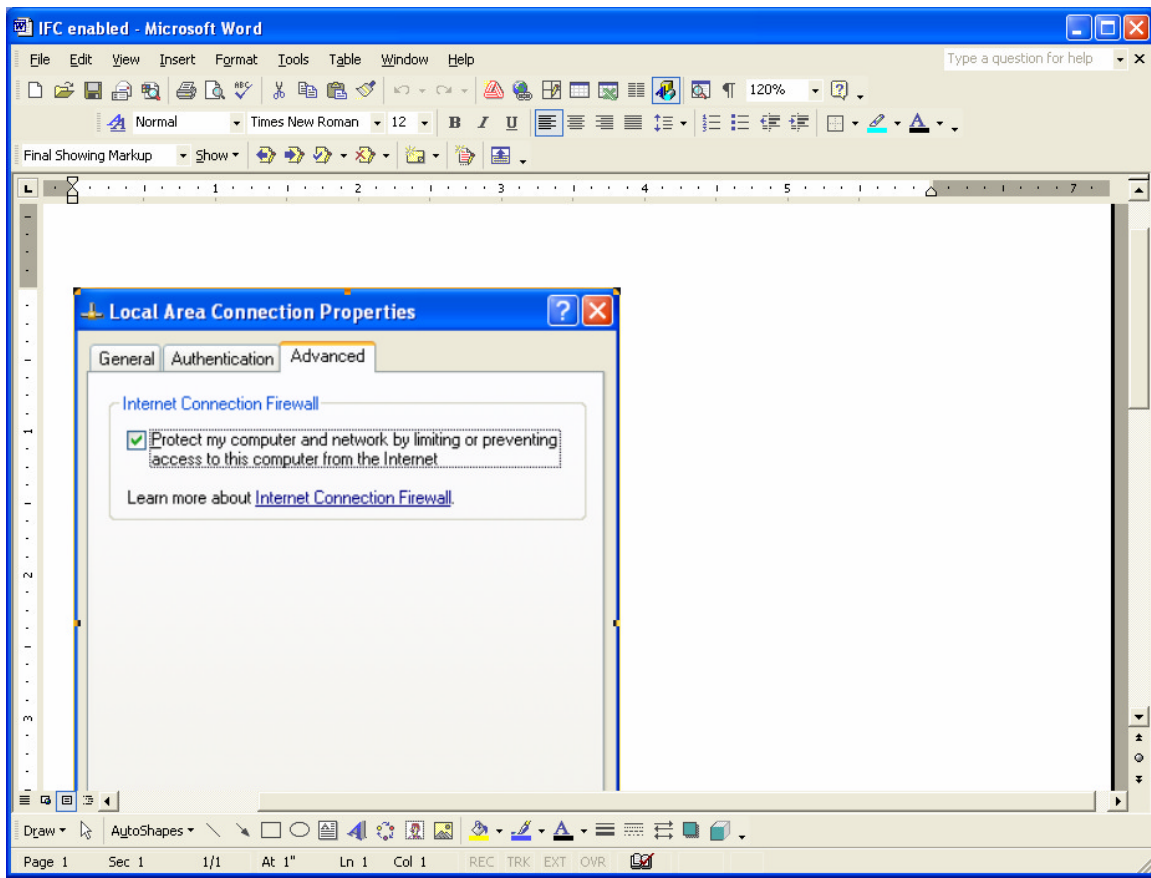
Additional Information

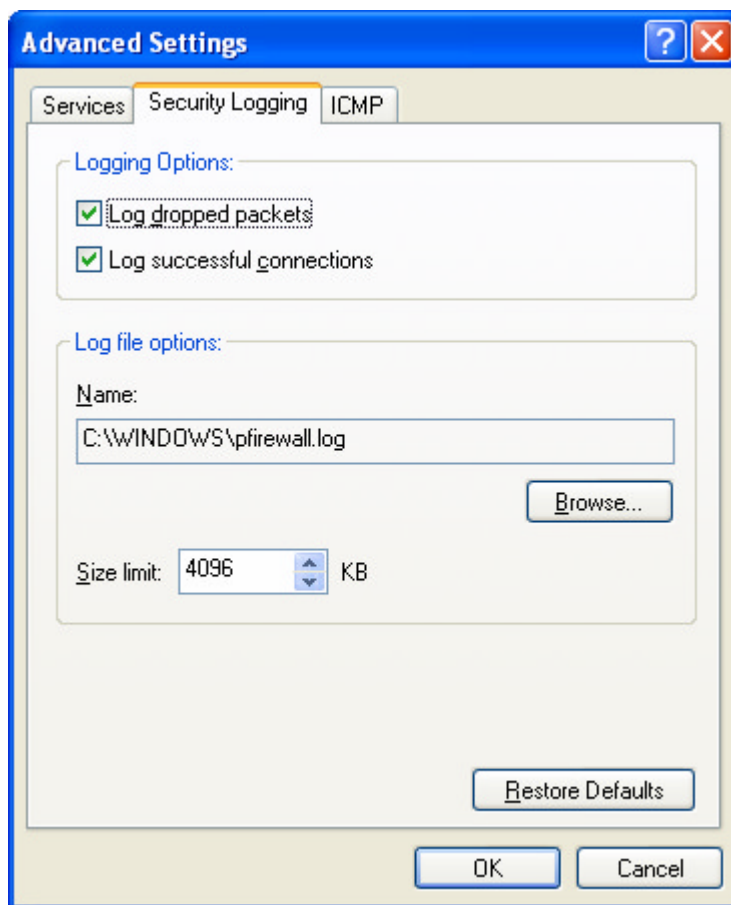
- [Microsoft Internet Explorer Unspecified CHM File Processing Arbitrary Code Execution Vulnerability \(bid 9658\)](#)
- [TrendMicro: PHP.Bizai virus description](#)
- [Description of Internet Explorer Security Zones Registry Entries](#)

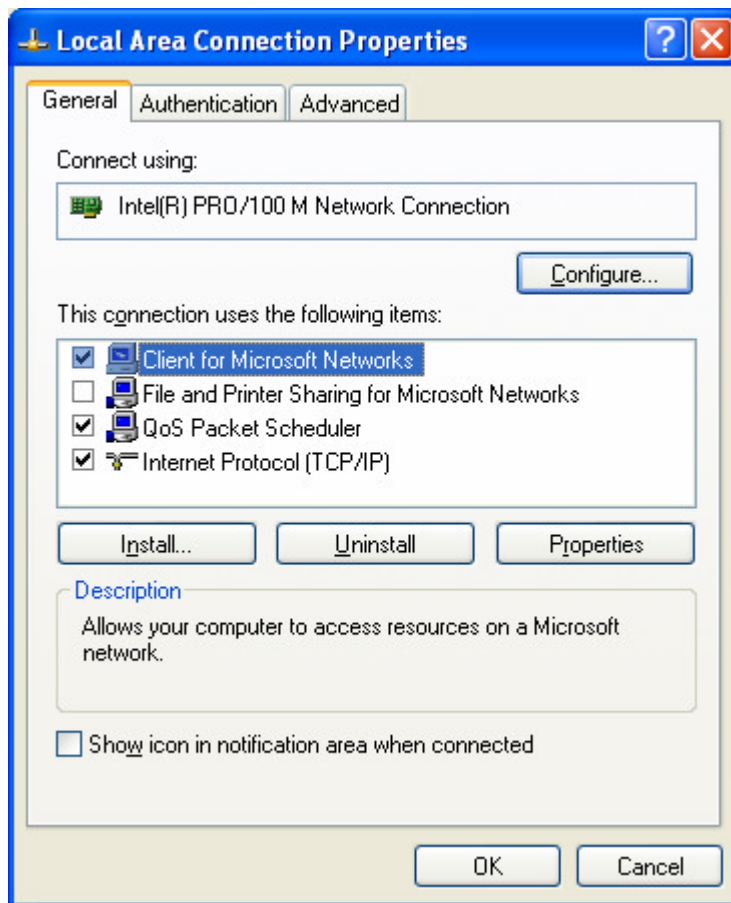
Appendix J

Microsoft IFC configuration

© SANS Institute 2004, Author retains full rights.



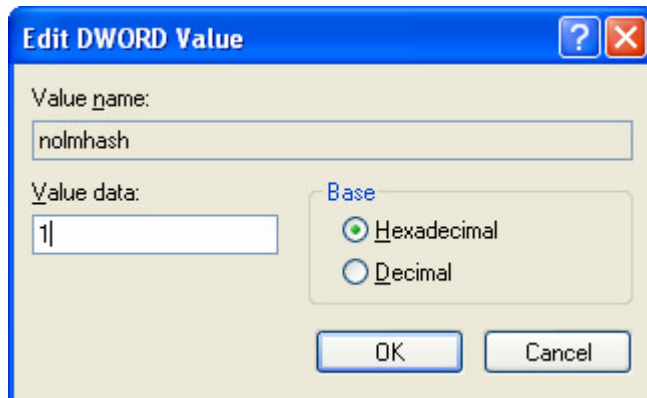




© SANS Institute 2004. All rights reserved.

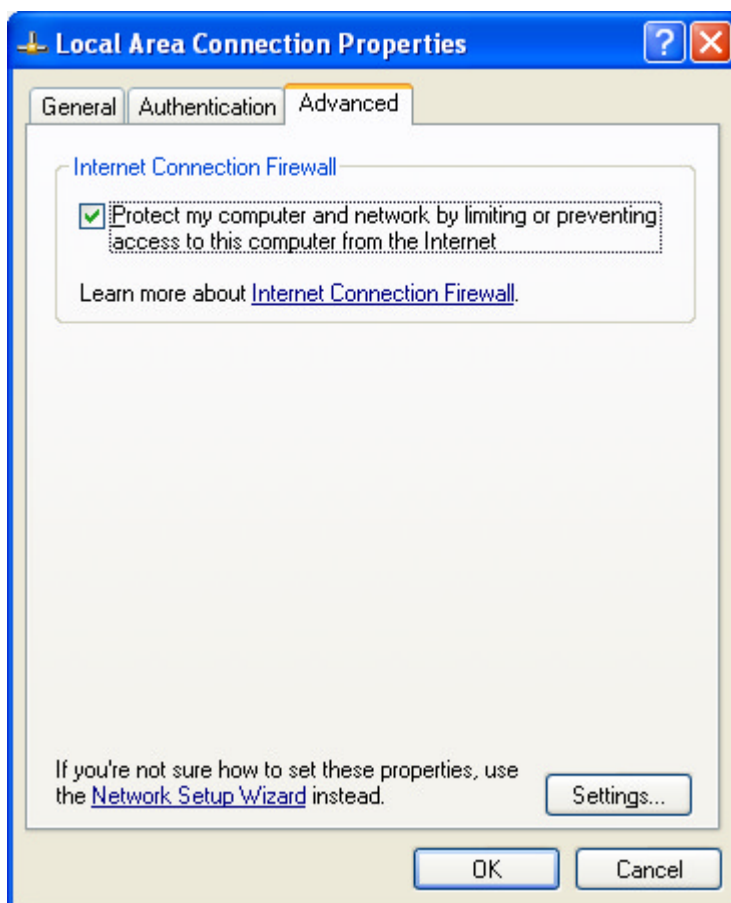
Appendix F

Lan Manager Registry Settings



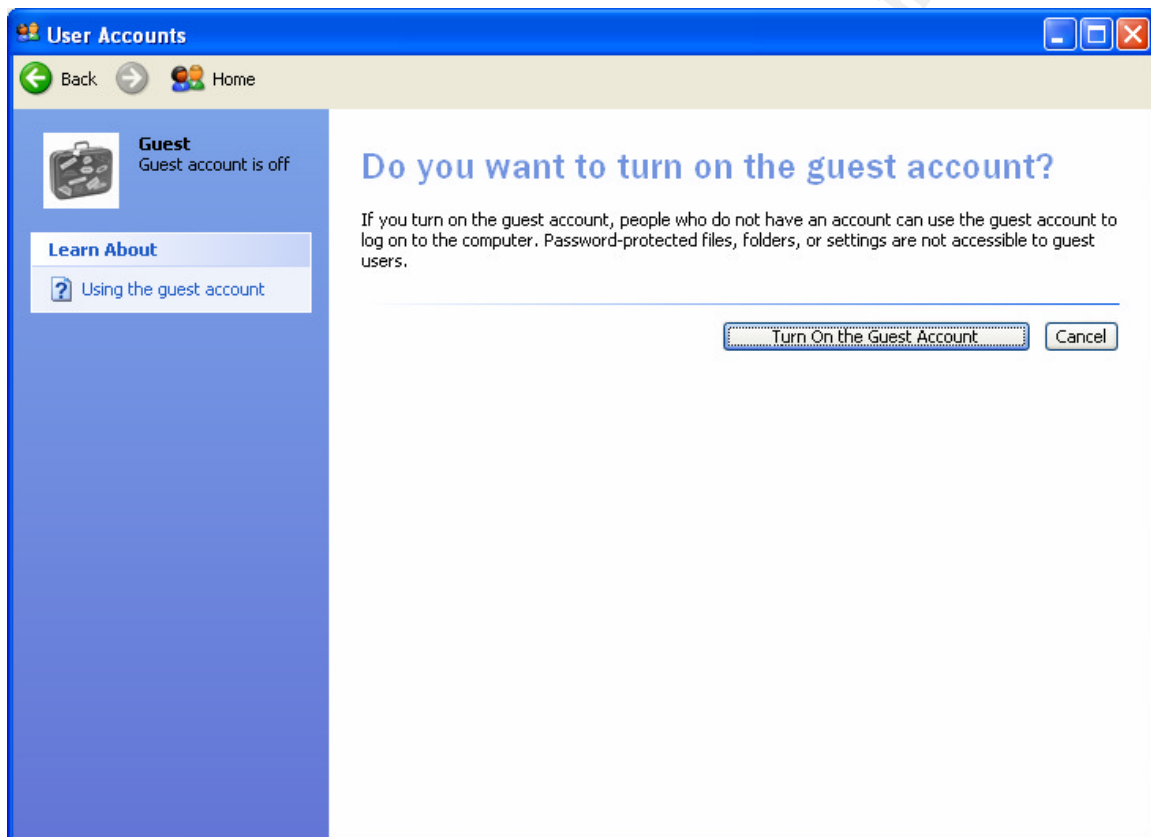
Appendix G

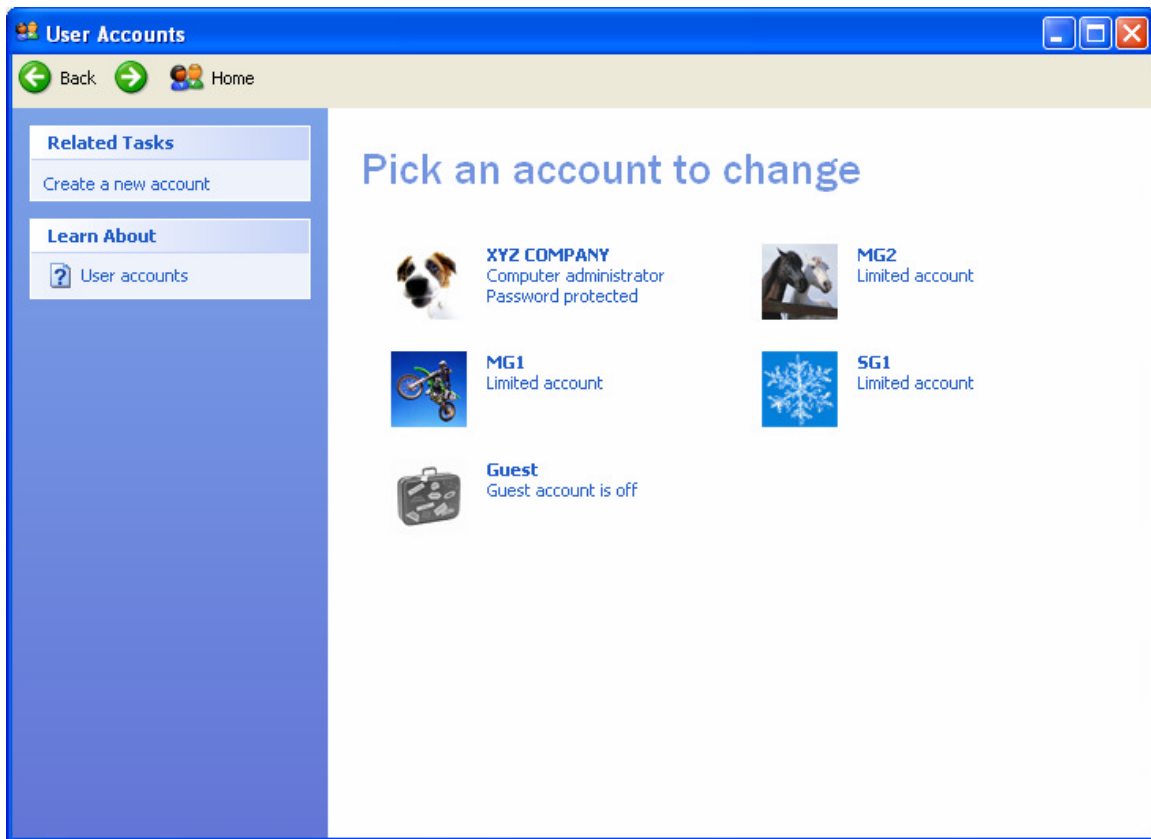
Microsoft Internet Connection Firewall enabled



Appendix H

User Accounts





© SANS Institute 2004, A