

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 permited without express written permission.

Security Audit Of A Consultant Windows XP Laptop:

An Auditor's Perspective

© SANS Institute 2004, Author retains full rights.

GSNA Practical
Version 2.1

By
Kevin Fuller

November 20, 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Introduction 4

I. Research in Audit Measurement, Practice and Control 5

2. Research 5

2.1 The Target System Configuration 5
2.2 Windows XP Overview 6
2.3 The Enemy: Facts, Figures, and the Threat 6
2.4 Current Trends in PC/Laptop Security Auditing 9

3. Risk Analysis 12

3.1 Physical Risk Analysis 14
3.2 Windows XP Risk Analysis 16
3.2.1 User Account Risk Analyst 18
3.2.2 File System Risk Analysis 19
3.3 Application Risk Analysis 20
3.4 Network/Internet Risk Analysis 22

II. Create The Audit Checklist 23

4. The Audit Process 23

4.1 The Audit Criteria 24
4.2 The Audit Checklist 24

III. Audit Evidence 49

5. Performing The Audit 49

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.1 Physical Security 49
5.2 Windows Security 49
5.3 User Account Security 52
5.5 Application Security 55
5.6 Network/Internet Security 57
5.7 Conclusions 61
5.7.1 Security 61
5.7.2 The Audit Process 62

IV. Follow-Up 63

6. Follow-Up of a Consultant Laptop Audit 63

6.1 Executive Summary 63
6.1.2 Audit Findings 64
6.2 Recommendations 65
6.2.1 Compensating Controls 65
6.2.2 Costs 65

APPENDIX A: References 67
APPENDIX B: Configuring and Using Microsoft 70
Security Analysis and Configuration Tool: 70
APPENDIX C: TCP/IP ports 72
APPENDIX D: Windows XP Security Features 75
APPENDIX E: Common BIOS Security Settings 80

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Introduction

I will be auditing the laptop of an independent IT consultant. Like many independent and small business consultants, his daily work world must revolve around his laptop. By necessity, he needs to connect to various client networks to do his job. Many of these small to medium business clients don't have the resources or the wherewithal to provide the consultant with a PC and a network login. So many consultants like him must use their own laptop to support the client, do their own work and to keep in touch with their consulting business.

The consultant's laptop uses the Windows XP Operating System. Windows is currently still the most popular operating system. While Linux continues to make inroads on that market share they are still are not as popular as some would wish. He has installed antivirus software, a spyware prevention utility and a software-based firewall as additional preventative security measures. He also has installed Microsoft Office as the standard application suite. My checklist will be to a document that covers the security of the laptop, Windows XP, Office, and the common security applications.

Since their inception, laptop computers have been a boon to computer users. Laptops free up users from their desktops and provide them with a means to do their work almost anywhere and have similar functionality to working at their desk. As technology has advanced, more power and functionality has been built into laptops, including better video displays, faster CPUs, more memory and drive space, internal modems and network interface (NIC) cards. These improvements have made laptops quite literally a replacement for the desktop computer. Now, with the advent of wireless networking freeing the leash to wired network and internet connections, laptops are poised to become the platform of choice for anyone who feels they want or needs computing portability in their business and personal lives.

However, all this portability comes with a price for laptop users and the business world in general - security risks. Being exposed to numerous uncontrolled and unfamiliar physical environments invites theft and unauthorized access. The ability and, in many cases, the need and or desire to connect to various networks and internetworks invites numerous risks. These include computer viruses and the spread of computer viruses, unauthorized access through hacking, backdoors, malware and social engineering. Theft of personal and company information through these avenues can result in financial losses, ruined reputations and diminished trust for companies and individuals at the center of a security incident.

I will first review the laptop configuration and its role in the consultant's business. After a short review of Windows XP I will delve into the some of the current trends and incidents in the business world as they relate to the threat to the average consultant. Next, I will identify the risks to a typical consultant's laptop and evaluate the specific impacts. Then, I will review some of the current trends in laptop security auditing and identify the resources I will use in my audit checklist.

I will then identify some specific audit criteria used in my checklist and create my checklist. I will next perform an audit of the consultant's laptop using the checklist. In the last section I will review the audit and make recommendations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I. Research in Audit Measurement, Practice and Control

2. Research

I will to create a checklist that will address and audit the secure configuration of a laptop used by a small business consulting firm or an individual consultant to perform his duties supporting business clients. This checklist will address the most common hardware and software components and security issues related to them in this category of laptops.

2.1 The Target System Configuration

An independent network consultant uses the system I choose to audit. In the performance of his normal work routine he logs on to customer networks to perform network troubleshooting and analysis. He uses software tools on his laptop to perform some of this type of work. He also downloads data files from customer networks and uploads files to their networks. He utilizes customer networks to access the Internet and his email in order to support his customers and his business. He creates documents on his laptop to support his customers. They can contain proprietary customer information.

The customer laptop configuration is a Pentium III, 500 MHz. It includes a CD-Rom drive (but no floppy drive), Parallel, serial, USB and Infrared ports. Also included is an Ethernet/modem PCMCIA card. Windows XP is installed and the following standard applications.

- Microsoft Office
- Microsoft Internet Explorer
- Microsoft Outlook
- Firewall Software (Zone Alarm Pro)
- Antivirus Software (Norton Antivirus Professional 2004)
- Anti Spyware software (Spyware Blaster)

In order to maintain control of the scope I chose not to address any additional applications in this paper. In reality, most additional applications installed will vary with the nature of each individual consultant's or consulting business's support offerings and expertise. This audit checklist will validate the security of the core software normally installed.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.2 Windows XP Overview

After having failed to merge Windows NT and Windows 98 together into Windows 2000, Microsoft decided to try once again. The result, released on October 25, 2001, was Windows XP. A hybrid of the two operating systems, Windows 2000 and Windows 98, Windows XP combined the best of Windows 2000's networking and security with Windows 98 graphics and multimedia capabilities as well as a whole new group of features. Several new security features were introduced in an attempt to improve on security shortcomings. Appendix C is a short list of those features (34).

All of these features combined with a more robust "default deny" approach Microsoft took in developing Windows XP to make it a more secure operating system than its predecessors. But, it is still along way from being highly secured as witnessed by recent events. The well-known Raw Sockets vulnerability that has been the subject of an on going controversy and the more recent RPC DCOM vulnerability that spawned this summer's msblaster attack are examples of security issues that continue to plague Microsoft products. To date, this year alone, Microsoft has released 41 patches to address issues related to Windows and Windows component security. They continue to take substantial criticism for their level of product security.

In the wake of this criticism, Microsoft has reviewed its 2001 security initiative and plans to refocus its security strategy. Their position is their products are secure when configured using their solutions and standards in addition to industry solutions and standards. To that end, they want to take their security mindset the network perimeter. It remains to see if they will be more effective or will continue to have the same difficulties that have led them to their current predicament .

2.3 The Enemy: Facts, Figures, and the Threat

As in all computers, there are many various security threats to an average laptop user. These threats however, are more diverse than those of the laptop user's peers who operate in a standard PC network. For the independent/small business consultant, they are exponentially greater. Working on a variety of networks with varying security profiles increases the exposure to a consultant. The threats come in all shapes and forms and create costly and expensive consequences to end-users and companies alike.

Perhaps the number one threat to laptop security is theft. It ranks second to accidental damage, but first among security-related losses (591,000 incidents) reported in a 2002 insurance group survey.(2) In a 2003 CIS survey of 530 security professionals there were 250 reported instances of laptop theft which accounted for 6,830,500 dollars in cumulative losses!! Compare this to the 2002 CSI survey where 503 security professionals reported 222 incidents totaling of 11,766,500 dollars in total losses. More incidents but, less monetary loss(3,4) In addition, other incidents serve to highlight the problem even more:

- In February 2000, the State Department reported that a laptop containing highly classified information was stolen from a conference room in the State Department Intelligence and Research Bureau building. On it were documents containing weapons proliferation issues with a "code-word" level of security which is considered higher than secret. The FBI is investigating the incident.(5,6)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- In July 2001 the FBI reported to the Department of Justice (DOJ) that a total of 184 laptops of various security levels missing from its agents or offices and at least 13 confirmed as stolen. This triggered a Department wide DOJ audit that resulted in the FBI having to own up to 317 missing laptop computers with 217 of them listed as classification status "unknown".(7,8)

- One of the more notable thefts occurred when Qualcomm CEO, Irwin Jones had his laptop stolen from a conference room where he was giving a briefing. Several documents with proprietary information were on the laptop and were considered of "high value" to foreign governments. (9,10)

- Recently, in Philadelphia, a Department of Homeland Security employee had his laptop stolen while training airport screeners. He had taken the precaution of insuring the front door to the meeting room was locked when they went to lunch. But, he neglected to check the back door. On the computers hard drive? Sensitive details about security at the nation's 429 airports! (11)

The CSI/FBI Computer Crime and Security Survey has reported that Laptop theft remains at above %60 percent of all incidents reported in its annual surveys. (45) The average laptop thief will usually fall into one or both of two categories. The first considers the laptop itself to be the goal. The high resale value makes the laptop a valued commodity anywhere from eBay to a local swap meet or garage sale. His only interest is the device itself. What is on the laptop's hard drive is secondary to the value it can bring reselling it

The second category of thief is more interested in the document and user account information and its value. Perhaps he is the interested party, or maybe he's interested in selling the information to interested parties. Corporate and government espionage is on the rise and a stolen laptop is easier to work with at one's leisure rather than probing your target's active network looking for holes in security. The FBI in 1999 estimated that 57% of computer crime was linked to stolen notebook computers. (13) With several keys to the castle in front of him the bad guy has but to obtain one password and he can access the company network.

The Gartner Group reports that 10-15% of laptop thefts fall into this second category. (19) Either way, the portability of laptops and the lackadaisical attitude most users have towards security contributes strongly to this growing trend.

The second biggest area of concern to laptop security is theft of information. The loss of the laptop is a concern for most individuals and companies. However, the potential loss and/or misuse of the information that is contained on laptop's hard drive is far greater and more serious. The 2002 CSI survey put the average loss from a laptop theft at about $89,000. (3,11) With the actual cost of an average laptop at about 3000 dollars it's easy to see that the information is exceedingly more valuable.

With the implementation of HIPAA (Health Insurance Portability and Accountability Act) and bills addressing compromised personal information like Ca SB1386 (15), the liability to companies and governments over stolen information in the commercial sector can only increase. SB 1386 in particular was a direct response to a highly publicized incident of information compromise in involving the State of California's Teale Data Center.

And then there's 9/11. Information compromise was not a big part of what happened that day. Its aftermath brought to the forefront the need to secure important information; how lacking the business and government really was at doing so and how much was really going on behind the scenes in the war in

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

cyberspace. Hackers are increasingly trying to gain a foothold into corporate networks to steal information or to just plain disrupt particular networks or the Internet as a whole.

The third biggest threat to laptop security – hacking - presents the threat with the most potential for unnoticed damage to laptop users themselves and to the networks they connect to. Hackers take advantage of security holes in operating systems, applications or email software. They use malicious software code like Trojans and backdoors to gain access to computers. Once they access the computer and compromise the security they can transfer important information like names, addresses, passwords, social security numbers, and credit card numbers from that computer or from other computers on that computer's network that they can compromise.

What's more, their compromise may go unnoticed for a long time depending on the sophistication of their attack and the tools they use. In California, The Teale Data Center recently discovered a compromise of one of its servers. During the ensuing investigation, they determined that the computer had been compromised for months prior to the discovery. At risk was the personal information of thousands of state employees. To date it has not been determined if there was any actual information theft.

Many times the compromise is to support plain focused or random destructive behavior. Gibson Research was recently a victim of a Distributed Denial of Service (DDOS) attack by a hacker using "bots". Owner Steve Gibson did some investigative research and reverse engineering of the attack. He determined that he had been attacked by a 13 year old in Wisconsin. The hacker had used a "bot", a piece of remote control software code, to take control of 474 poorly secured computers attached to the Internet. He then attacked GRC.com with those 474 computers using a Distributed Denial of Service attack, not once, but several times.

The hacker's reason for this attack?

He did not like something Steve said about hackers in an Internet chat room. (16)

Hackers are not the only users of these types of programs. Legitimate businesses and governments with an interest in learning information about their customers, Internet users in general or advertising their products are another category of users looking to compromise computers and networks. They use cookies in Internet Explorer, or "spyware" to gather harvest information about users and their browsing habits. Popups, cookies and spam email attempt to interest users in the company's products or services. Annoying at least, and a serious compromise of security at worst, they present a different variation of the hacking threat to laptops as well as computers in general.

Viruses present another threat to laptop security. Malicious code created and designed to disrupt computer operations, they commonly are delivered by email or infected files. They can do as little as display an annoying message or be as destructive as deleting files or doing mass mailings of themselves using the targets address book. In most cases, the behavior serves one general purpose, to disrupt computer use and computer-based communications. That is, until recently. The recent virus attack by msblaster carried an additional threat. The virus is reported to carry an additional payload of Trojan and back door programs designed to compromise target machines. (17) So now one may cleanup the virus infection and still be vulnerable because of installed, undiscovered backdoors.

So what does all this threat mean to the average independent consultant or small business consulting firm?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As mentioned earlier most consultants will have to, by the nature of their work, spend more time traveling than most people in order to reach customer sites. They will connect to these various customer networks. The number of networks involved multiplies the risk over that of a desktop user or even an average laptop user. Since the consultant has no direct control over the customer network, he has no assurance that the network he is connected to won't compromise his laptop.

When put in this same situation a small business consulting firm now has this magnified by the number of consultant laptops they possess. If a laptop is compromised and undetected it can, in turn pass that compromise to the firm's network. This compromise can then be transmitted to the other consultant laptops and through them to other customers, to business partner networks, the threat expands exponentially very quickly.

How can one defend against the threat?

Quite simply, self-preservation. In other words, ensuring that the consultant laptop is secured to the highest possible degree against compromise.

2.4 Current Trends in PC/Laptop Security Auditing

From my research and personal experience in the corporate world, the need for auditing end-user PCs continues to more of a reactive rather than a proactive activity. There are plenty of white papers, reference articles and guides on what to do to secure a laptop against theft and compromise. In large corporations there are security policies, emphasis on antivirus software, user security and accountability, perimeter security and auditing and other general responses to the need for security. In many cases, there does not seem to be a lot of follow-up that periodic system auditing would supply. In smaller businesses there is even less concern for security. This environment consists of unsecured modem connections, some or no antivirus software, little physical security, and unlimited access to the Internet. In addition, there is very little oversight for what is introduced or is installed on a computer. In both worlds the requirement to update and or patch operating system or application software on computers runs headlong into overworked staffs (corporate) or falls (in small business) to the employee who knows the most about computers (and little about the importance of patching).

That is until an incident occurs. A virus infection impacts the network and computers on it. A compromise of the network by a hacker is discovered. The network and/or computers on it go down because it is being subjected to a denial of service attack. Or worse yet, the outage occurs because the business's computers have been compromised and are participating in a distributed denial of service attack on someone else's computer or network!

Once the initial incident is addressed and resolved, most companies will overreact in their attempts to prevent a reoccurrence. Bordering on overkill, the IT staff/person/consultant are now directed and motivated. The perimeter is locked down. Aggressive and unfettered patching of PCs and software begins. Antivirus software is installed and/or updated. The Internet Use is restricted. In the end, the security profile of the business is heightened. With luck it, it will stay that way and the lesson is learned.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Take, for example, Beth Israel Deaconess Medical Center (BIDMC) in Boston, a Harvard University research institution. When the Slammer SQL vulnerability was first announced they patched their SQL servers and left it at that, satisfied they had covered their bases. When the Slammer virus hit it found an avenue - the Microsoft Data Engine on unpatched Windows XP desktops.

After 6 hours of down time and numerous hours of overtime the hospital's Chief Information Officer (CIO), John Halamka was satisfied that his security vulnerability was fixed and his security profile was as high as it could get and he was determined not to let it slip. When the Microsoft RPC vulnerability was announced the hospital's IT staff immediately patched and reconfigured their perimeter devices to detect and deny a virus attack. They then went on a "nightmare-a-thon" patching desktops and servers. The result: their exposure to the msblaster virus was both limited and controlled. The culprits who were responsible for the limited exposure were two employee laptops had acquired it through a home Internet connection before connecting to the hospital network. (1)

This highlights a critical issue with laptops and the need for proactive security auditing. Portable laptops are just that, portable. The mobile users may not visit the business campus for weeks on end limiting the IT staff's access to the laptops. Infrequent attendance also ensures that the laptops may not get updated or reconfigured when needed.

In fact, most mobile end-users are more concerned with getting their work done than keeping up on the patching and configuration of the security. In many cases, the less security involved, the easier it is for them to do their jobs.

In addition, most users are also administrators on their laptops and have the ability to change security settings at will or install whatever software, legal or not, they feel they need. They may attach the laptop to their home Internet connection or to a friend's home network without thought to the security consequences of that connection. With independent or small business IT consultants the patching and updating may be less of a concern as they may be a little more diligent than most. The software issue may be more of a concern. In their quest to find the "tools" to do their job that they otherwise don't have but feel they want or need the consultants may procure freeware "hacked" or "warez" copies installed from questionable sites that the may know of. Translated, that means higher exposure to a potential virus or hacking infestation and licensing issues.

When preparing for any audit it is important that the audit conforms to standards at different levels in order to lend validity to the outcome. To just decide that this needs to be audited this way or that needs to be audited that way does not lend a lot of creditability to the audit. There are numerous standards organizations and source documents that will give you the necessary foundation. A few of these are:

ISACA: The Information Systems Audit and Control Association provides international standards and the COBIT (Control Objectives for Information Technology) guidelines, Control Objectives and a process model for Information Technology systems and auditing. They provide a high level framework and both general and more specific guidelines that one should meet to define a complete and standardized Audit program. Many of the guidelines are too high level and inclusive for an individual or a small consulting business to utilize effectively. Nonetheless, I attempted to follow the framework whenever possible.

NSA: The National Security Agency. Provides several guides that layout detailed standards for networks, network components and computer Operating Systems.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CIS: Center for Internet Security has created benchmark documents based on the NSA standards for Cisco IOS, Windows and Unix/Linux. They have also created some scoring tools that can be used to automate the assessment process to determine if the subject OS configuration meets NSA standards.

SANS: System Administration Network Security. The SANS/FBI Top 20 Vulnerability list addresses the most current and substantial vulnerabilities and how to address them. It provides a good starting point on what specific threats should be considered first in securing networks and computers. They also have numerous documents and ongoing projects posted on the website by contributors related to all facets of security, including auditing.

GIAC: Global Information Assurance Certification. GIAC is the certification arm of SANS and deals with certifying security professionals. More importantly from an auditing prospective, they post the student's written practical on their website. The equivalent of a thesis, each paper must conform to the current standards, guidelines and published best practices for the chosen subject within each SANS track. In auditing, this means that each posted practical will address some level of auditing policy or some level of auditing practice on selected equipment or IT solution. This will provide one with a great, validated foundation from which to start from when developing an audit.

NIST: National Institute of Standards and Technology. NIST is the Government agency responsible for establishing and publishing national standards for business and industry. They maintain a library of standards-based Computer and Network Security guides and checklists.

Microsoft Corporation: While Microsoft is regularly lambasted about the insecurity that seems commonplace in their software, little mention is made of their follow-on security programs and their published security guidelines. A correct search of their website usually brings back a number of documents related to security settings and security best practices. Taking these documents and making a positive effort to implement their recommendations can go a long way to securing the Microsoft operating system and application software. The keyword here is best effort!

My research has revealed a number of papers on the topic of laptop security. A vast majority of them focus on the issue of physical security of laptops. Others combine physical security with operating system security but do not address either with any degree of depth. Likewise when it comes to addressing Windows and Windows XP many papers do not cover the broad spectrum of security settings that Windows has.

There is also little out there that I could find (outside of Microsoft) that delves into the granular security settings of Windows and the use of the Microsoft tools like Security Configuration and Analysis tool and Microsoft Baseline Security Analyzer. These two very powerful configuration and analysis tools can lighten the workload of securing Windows. In preparing the audit checklist I choose to use the following resources and my personal experience for most of the of the checklist items. I will work to create a checklist that combines the best of both Laptop and Operating System/Application security, with other areas and material I have researched into a comprehensive audit plan for laptops and consultant laptops in particular.

1. M**icrosoft Windows XP Security Guide:** This document is a comprehensive guide addressing the security settings available in Windows XP through the Security Settings, Group Policy Manager and Security Configuration and Analysis Windows components. It provides a brief

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

explanation to the why and how of each setting and three recommendations based on individual environments.

2. **Microsoft Personal Computing Security**: a series of papers addressing security settings, maintaining security, passwords, firewalls and a 3 part step by step guide to the Windows firewall , updating software and antivirus protection.

3. **SANS/FBI Top Twenty Vulnerabilities**: A list compiled by SANS and the FBI of the top ten Unix/Linux and the top ten Windows security vulnerabilities and fixes for them.

4. Labm**ice.net Windows XP and Laptop Security Guides:** Each guide from this Windows Resource website addresses the more common and some uncommon general security issues and has some recommended remediation for each.

5. **GIAC contribution paper Mobile Computing Self Assessment for Non-technical Business Users, Micheal Hagerty**: A good general laptop audit reference addressing the laptop and the installed software.

6. **GIAC contribution paper Methodology for Auditing The Windows XP Operating System, Tony Howlett**: One of the few papers that addresses the Windows XP security guide recommendations

3. Risk Analysis

Risk analysis begs the question "How likely is it that it could happen to me/us?". What is the impact of it if it does happen? Well let's step back and look at what may be an average day for an independent consultant.

He starts his day with a trip to the airport to fly out to Boondoogle, Ca to do some consulting for some clients. On his way, he stops at the Quickstop for gas and a cup of coffee. He leaves his car unlocked while he runs in quickly. Maybe his laptop is in his back seat, maybe it's in the trunk. He gets to the airport and jumps on a transit bus that will take him from parking to the terminal. He puts his luggage and laptop in the luggage rack and takes a seat. When he gets to the terminal he has to wait in line to check in.

After 30 minutes of shuffling through the check in line he sets his gear down and goes over his reservations with the ticket agent. He checks in his luggage and heads to his gate to wait for his flight.

At the security screening section he puts his laptop bag on the x-ray scanner and proceeds through. After being hand screened because he set off the metal detector, you grabs his laptop and heads for his gate. He decides to stop at the wireless Internet café on the way and check his email. While waiting for it to download to his laptop through the café's wireless access point, the consultant gets up and takes a few steps to the bar to get another cup of coffee.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

He takes a few minutes to read his email and then packs up his laptop and heads for his gate. On the way he bump into a lady in hurry and knocks a stack of paperwork out of her hands. He sets his stuff down to help her pick them up. He gets to his gate and sits down only to be called to the check-in counter by a gate attendant. After talking to him he decides to relax and read the paper until his flight is called.

It's a crowded flight and he has to store his laptop in an overhead near the back of the plane (his seat is in front). He arrives at his destination and heads for baggage claim. When the baggage turnstile starts, he gets up from his seat and waits for his bag. After a trip on another one of those airport transit buses you sets his bags down at the car rental place to talk to the rental clerk. he gets a car and you're on his way.

His first stop is ABC Company. They have long had a low security profile and now they have the blaster virus on their network. They want the consultant to clean it off and help their IT person to patch and update his network. The consultant logs in from his laptop with his assigned account and begins work.

From his workspace location the consultant ends up actually walking to some office locations to work on pieces of the network. At a new client the IT person is gone so the owner gives the consultant the administrator account and password to get on the network and do some basic administration

Another client is building a call center and they want the consultant to look at some of a contractor's work on the servers and cabling. His last client of the day owns a firm that created a "white hat" hacking program. He has some problems with saturated bandwidth he wants the consultant to look at. While working on it the client calls the consultant into the office to ask him about on another issue. After finishing his work the consultant heads back to the airport for another round of the airport shuffle as he heads to another city and another day. Maybe he can grab a catnap in the terminal or on the plane.

So with his day done; how much risk was there? Or how much risk could there be in a typical week of days similar to this one? Lets look at a summary of the risks this consultant encountered in his day and then break each category down.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following matrix is columnar in format. By picking the threat in column 2 and it's corresponding likelihood of occurrence (column1) and applying it to the situation(s) in column 3 one can determine what risk area(s) in column 4 are impacted and map it all to the outcomes in column 5. Since there are direct and indirect as well as one to many cause and effect relationships in the Risk model this chart will work in mapping them.

Summary of Risks

Likelihood Of…	A threat such as…	Could occur...	and affect one or more risk areas...	and will result in…
High	**1** Theft of Laptop	At the Quickstop (1,7)	Physical Security	Loss of propritory information
High	**2**. Introduction of a virus	While on the bus(s) (1,7,9)	Windows Security	**Financial liability for consultant**
Medium	**3.**-Introduction of backdoor	While in line(s) (1,7)	*User Account Security	* cost of replacing laptop
Medium	**4.** Introduction of a Trojan (Backdoor)	At the ticket counter (1,7)	*File System Security	* cost of replacing installed software
Low	**5.** Unauthori zed access (social engineering)	At the airport security check (1,7,9)	Application Security	* Legal costs related to possible client litigation
Medium	**6.** Unauthori zed access (hacking)	At the internet café (1-8)	Network Security	*Lost business income
High	**7.** Loss of information (Theft)	At the airline gate (1,7)	Internet Security	Loss of trust impacting consultant reputation
Medium	**8.** Loss of information (hacking)	While helping the lady in the airport. (1,7)		**Financial liability for client**
Medium	**9.** Loss of information (Physical damage)	While on the airplane. (1,7,9)		* Cost of repairing the network and/or computers (IV,)
Medium	**10.** Denial of Service	At baggage claim (1,7,9)		*Cost of replacing lost information
		At the rental car counter (1,7,)		*Loss of business from loss of trust in client
		While connected to the customer network (1-8,10)		*Loss of business from possible loss of necessary information
		While away from the desk at the client site (1-10)		*Legal costs related to possible customer litigation
				*Legal costs related to possible consultant litigation

3.1 Physical Risk Analysis

Physical risk implies that the bad guy is actually able to place his hands on the laptop and/or be able to access the power switch, keyboard and mouse. We stated earlier that theft is the number one threat and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

accounts for a majority of the losses of laptops in today's world. Looking at our consultant's typical day shows why this is the case. The risk of threat is prevalent in almost all the situations in Column 2. Without proper physical security controls and awareness there are many opportunities for his laptop to get stolen. In the car, any time he needed to set it down to do something else or was separated from it. This is what thieves are counting on. Recent articles point out two scenarios being used to separate users from their laptops long enough for them to be stolen.

In the first, a two-man team marks their target (you) at the security screening area. One person gets screened and waits. The second person waits until you've placed your laptop bag on the X-ray scanner belt. At this point, he then manages to go through the metal detector ahead of you and set it off. While the screeners are busy resolving his issue and you wait patiently for them to finish, his partner has grabbed your laptop and is headed away from the area.(18)

In the second, the pretty lady marks you as the target. She smears mustard on your shirt without your knowledge. She then stops you to point out the stain and pleasantly offers to help you clean it up. She's counting on you to put you laptop bag down to accept her help, at which point her partner will spirit it away while you are occupied with her. (27)

In addition to the above threats, numerous opportunities exist at the work site while you are working on your laptop. If you have to step away from your desk for a meeting to do some work in another part of the office or to simply take a lunch break, you invite the strong possibility of theft of your laptop. As a contractor you are not considered to be part of the company. A line of logic may exist that might encourage others to consider it OK to steal your laptop. How does one control the possibility of theft? The following are the controls that can mitigate the possibility of theft.

1. **Security awareness:** Being aware of your environment and the threat.

2. **Labeling your laptop bag:** Marking pen, reflective tape or even a simple exposed or hidden luggage tag can make a difference.

3. **Secure your laptop bag**: A cable and lock combination threaded to the bag handle and/or luggage locks on the zippers to the laptop compartment of the bag are a minimum solution to deter quick and easy theft. At the high end, several companies have designed security systems that will audible alarm if you (and the receiver) are separated from your laptop bag (and the transmitter) by more than a certain distance.

4. **Labeling your laptop**: 97% of unlabeled laptops are never recovered. (27) Several companies make tamper-proof asset tags that cannot be removed. This can discourage a thief, as a "labeled" laptop will be harder to sell. At the high end are software applets that reside on your hard drive's boot sector. Next to impossible to remove without reformatting the drive, they will "phone home" when attached to the Internet. A preprogrammed link to a site will allow the laptop to connect and download a preset set of information making recovery a strong possibility.

5. **Secure your laptop:** A cable lock with a cable attached to the micro-security slot of the laptop and to a table leg or other immovable object can prevent your laptop from sprouting wings in the office or the Internet café. At the high-end motion alarms that will alarm if the laptop is moved are the current product of choice.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The next facet of physical security involves physical access to the laptop. If your laptop is stolen or if you leave it unattended on a desk turned off. There is a high risk that the system could be booted and the drive accessed.

First and foremost is using the computer's BIOS to prevent theft or loss of data. With access to it options such as the boot up sequence can be changed allowing better access to the system. While not the most efficient of the security options it nonetheless is listed as a requirement in the NSA level 1 Security standard.

Most bad guys with computer experience know that even an NTFS file system used by Microsoft can be compromised. Use of a bootable floppy or CD can provide a default operating system environment. From there tools like NTFS for Dos can allow a hacker to mount and read the NTFS partition on the hard drive giving him access to all the important information. Tools like DumpACL, LC 4 and Jon the Ripper can access the SAM security hive of the registry and compromise the user accounts/passwords found. Controlling this type of access can include the following:

1. **Use a BIOS Password**: Most BIOS have an option to set a password to restrict access to the BIOS. If yours does, set it and make it a complex password. What is a complex password? It should be a minimum of 8 alpha and numeric characters and should not be based on a common word or phrase. There are tools available to compromise BIOS passwords. The more complex you make it, the harder it is to be broken.

2. **Use a boot password:** If your BIOS supports this option, then use it. It will prevent your system from being booted from any boot device. Again, use a strong, complex password. If not or, if you want an added level of security, you can look at the current generation of Biometric scanners that look at your eye's retinal pattern or a thumbprint to grant you access.

3. **Set your boot options to disable the floppy drive and the CD-Rom drive:** With both drives disabled as boot options they cannot be accessed at boot up with a bootable media. This will limit the likelihood of physical compromise of the hard drive.

3.2 Windows XP Risk Analysis

Window XP is a step in the right direction for Microsoft. After years of being hounded about their lack of security focus they are finally attempting to market products that are secure out of the box.

But, they have a ways to go before others can believe their claims of "secure" products. We discussed earlier some of the security features that Windows XP possessed. In spite of that, Microsoft has released 41 security bulletins this year to date and 72 of them last year.

The important distinction when working with Windows XP is the Local Security Policy and the Domain Computer Security policy. All of the secure setting changes we will be auditing are to the local computer only. As an independent consultant, you are exposed to numerous networks over the course of a month. Some may be ad-hoc or peer-to-peer networks, while others may be full-featured enterprise networks. Logging into a Windows NT or 2000 domain network will invoke additional security settings that may

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

supplement OR change the default local policy settings. Other, less robust or secure networks like peer-to-peer networks may leave one exposed to potential compromise unless the laptop settings are set to the highest security level possible.

No matter where you look on a Windows machine there are some security related settings that could be addressed. User accounts and file permissions are two areas (discussed in later sections), where the defaults are not highly secure.

Services installed and running that are not needed is another such risk. Steve Gibson of Gibson Research has highlighted many security issues regarding security issues such as Raw Sockets, Plug and Play and NetBIOS on his website. (21,22) Microsoft insists that some of these features are needed but, when disabled, they seem to have little or no effect on the operability of Windows.

How can you make Windows secure??

Don't turn it on?

Yes, but considering you have to use it, the next best way is: **PATCH IT!** Microsoft has always been good at learning about a vulnerability and then creating a fix. Beyond patching there are numerous other settings that can and some cases should be changed to increase security. Microsoft even has a collection of tools and templates to change security settings in mass. In the interest of scope, I will concentrate on the most obvious settings here. The checklist will address more settings

1. **Patch Windows:** The more current you are with patching, the less chance of your machine being compromised. Microsoft suggests automating the use of their Windows Update service to keep your Windows patches up to date. They suggest that you let it run automatically. I feel that, whether you are an individual consultant or a consulting business, you should not allow uncontrolled or supervised downloads to your hard drive. Not to mention that the potential for compromise through site redirection. Therefore, I recommend that you set it to run manually and notify you before starting a download.

2. **Disable unneeded services:** Services such as FTP, NetBIOS, Windows Universal Plug and Play, service and Remote Registry are not needed all the time. If they are needed some of the time set them to Manual rather than Disable and start them only when you need them.

3. **Enable the logon screen and set it to not display user name and not to save the password**: Having a logon screen forces you to enter a name and password and not use the autologon feature. A blank user name prevents the social engineering hacker from learning your userid or the naming convention for your computer or the network. Not saving the password removes a potential security hole that could be exploited in order to get the password.

4. **Disable autorun on the CD-Rom drive:** This will prevent someone from using an autorun CD to install a backdoor on your computer. Something that can be done as long as Windows is up and logged into.

5. **Disable USB ports when not using them:** This is more of a corporate desktop issue but, it can't hurt to be extra cautious. While I have not heard of it happening, I can just imagine a USB flash drive configured to execute a script file much like an autorun file when accessed by Windows during

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

initialization. That script could install a backdoor onto the system or download the contents of the My Documents folder. If the USB ports are not regularly, used why leave a possible security breach open?

6. **Enable Logging:** Tracking the activity in Windows can alert you to attempted or successful compromises and allow you to respond more quickly when they occur.

3.2.1 User Account Risk Analyst

User accounts on a Windows machine are the keys to the castle. The local administrator account allows full access to all of the Windows OS. The guest account has long been a backdoor to the local machine and through it to the network. If you log onto a network then domain accounts and passwords may be stored in the SAM database on the local machine. This is an even better set of keys to the castle for the bad guy. In all likelihood compromising user accounts has a strong probability of occurrence in a given day.

There are plenty of programs out there, which can extract the account and password information out of Windows and then crack the passwords or log keystrokes and within these keystrokes the accounts and passwords. An independent consultant will have a potentially higher risk than most. In our scenario the consultant had to log into a few different networks during the course of his day. Multiply that by days or weeks and it represents a number of network accounts. That means that, baring network level restrictions, his domain user account information for each was downloaded and stored in his laptop. If his laptop is stolen or hacked it represents a potential security risk and loss of information, trust and dollars for each company for which he has had to connect to their network with his laptop.

As with every other facet of security, there are ways to mitigate the risk:

1. **Disable the Guest account:** Windows XP disables this account on installation, but it doesn't hurt to check.

2. **Rename the Guest account, remove Group membership and account comments and set an extremely complex password:** Most hackers will look for "Guest". If they can't easily find it then their job is harder and more time consuming. Setting an extremely complex password (long, random numbers, letters and symbols) will ensure that, if the bad guy locates it he will have a hard time breaking it. If he breaks it he won't have rights to anything without an assigned group membership.

3. **Rename the Administrator account, set a complex password and remove account comments:** This is the same as the Guest account. A hacker will look the name or something that looks like it. Hiding the account with a generic account name makes it difficult to locate and a complex password will make it harder to crack.

   NOTE: Both (2) and (3) may require adding some dummy accounts to your computer with general group memberships and extremely complex passwords in order to better hide the real accounts

4. **Create a dummy administrator account with an extremely complex password and no or user only group membership:** This is a classic misdirect that should fool all but the most experienced hackers. Social engineering norms suggest that most hackers conclude that their targets do not

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

practice security. So, seeing an account named "administrator" or "admin" on a compromised machine will, most of the time, not strike them as unusual. Therefore, they will likely burn a lot of midnight oil hacking this dummy account only to find that once cracked, it gets them nothing.

5. **Disable all unneeded user accounts:** In their infinite wisdom Microsoft added a pair of desktop support accounts, HelpAssistant and Support_xxxxxxx . If the laptop comes from a major manufacturer they too have added a Support_xxxxxx account. They are disabled by default. Again, it doesn't hurt to check and, while you're at it, set an extremely complex password and remove any group memberships.

3.2.2 File System Risk Analysis

Windows file system is based on Microsoft's NTFS, a secure partition format that limits access to the drive without an NT-based OS like Windows 2000, XP or NT. In Windows XP there is an added enhancement, Encrypted File System (EFS). With EFS, folders and files can now be encrypted with 128-bit encryption key preventing access by anyone other than the designated accounts. Even with this, there still remains a risk to the file system and through the file system to the laptop drive.

Share folders provide a conduit through which the bad guy may find his way into a laptop. Folder and file permissions by default are not set to most restrictive, even if restructured correctly. A careless user with the best of intentions can change the permissions on a whole folder tree trying to increase or reduce the security on a particular file or folder. One the more plausible scenarios involves folder/file permissions and NetBIOS sharing. A folder shared as a network share with default permissions is wide open and can be accessed on the network by most anyone. EFS in XP uses a different method of encrypting a file or folder than Windows 2000 did. It is more secure than the previous method and provides an easier recovery methodology should the user lose access to their files. But the method does open up a risk to cracking the encryption or using the required password recovery disk if the bad guy gets his hands on it to access the files.

To address these issues one should look at the following basic steps:

1. **Evoke the most restrictive group membership on the file system wherever possible:** The Everyone group has somewhat more restricted access than the Users group. Authenticated User group membership may provide another level of security between group members and the file system, insuring they are authenticated before allowing access rights to files and folders.

2. **Evoke the most restrictive folder/file access permissions on the file system wherever possible:** Not every file and folder will need full control access to function properly. Wherever possible change to more restrictive permissions (ex. Read & Execute, Read, List)

NOTE: Both of the above may take some trial and error to determine the most restrictive but still usable security permissions for the file system, particularly the OS folders and application folders containing the application executables should one decide to limit access to them.

3. **Use EFS on the data file folder(s):** Designate a default document folder (Usually C:\My Documents), ensure that all applications that allow you to change their default file save locations

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

point their save function to that folder, then encrypt that folder with EFS. Encrypt the Temp folder to prevent access to document temp files. Use EFS to encrypt the folder rather than the files to limit the chances of decrypting the file using the "save as" function. Disable print spooling to prevent unsecured spool files from being created. Be sure that a password-reset disk and/or a digital certificate backup is created. One for each active user account on the machine. This will allow recovery of encrypted data files if the password /certificate is lost or corrupted. If you're a small consulting business, you need to designate Recovery Agents and develop recovery procedures as well as insure consultants are trained on using the EFS protected shares.(30)

4. **Restrict shared folders**: If shared folders are needed, enable sharing to the minimum number of folders and set the permissions to the most restrictive possible.

3.3 Application Risk Analysis

Applications are no less safe from compromise than any other area of a computer system. From the routine to the unique, they all are susceptible to exploits by determined bad guys. Even NMAP, a popular security vulnerability assessment tool, is vulnerable to an exploit of its Winpcap library. A consultant or small consulting firm will have a standard suite of applications plus various IT utilities necessary to support their customers. Then there are those applications necessary to support unique requirements of each customer. A good example of this would be a consultant/firm that may do web programming/support or database programming support as part of their service offerings. He/they may need to have a variety of web and database applications or utilities installed to support these functions. Both types have various documented vulnerabilities that would need to be addressed.

Microsoft's products, by virtue of their extensive use in the market, are the leading targets for those looking to compromise security through vulnerabilities. Chief amongst their product offerings is Internet Explorer. By tightly integrating IE to the operating system, Microsoft has opened up its browser to some of the same vulnerabilities that affect its operating system and many that are unique to the Internet. It is the Internet-based vulnerabilities where the most probability of risk occurs

Malicious code can be hidden in a web page accessed by Internet Explorer. Once activated, it can make malicious changes thru IE's hooks in the registry or its links in the Windows core file system (System and System32 folders).

Their email program, Outlook, carries similar vulnerabilities. Most of these are related to how Outlook handles attachments. Malicious code disguised as a ZIP, .vbs or like file type or a standard document with a malicious macro embedded can be part of an email. Once clicked on most email exploits will use the victim's address book to spread itself and the resulting infestation generates a bandwidth consumption attack.

Furthermore, Microsoft Office is host to several vulnerabilities that need to be addressed. Most of these are related to Visual Basic for Applications and Macros.

When evaluating security of applications, one must not forget some of the underlying engines that may be installed. For instance, Java and JavaScript engines, Microsoft MDAC and SQL client and other such

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

components may get installed as part of application software used by the consultant/company and are easily overlooked. To do so invites disaster to occur much like the Boston Hospital in our first example.(1) Many times, the user doesn't even know it's been installed. Many consultants were very surprised to learn they were vulnerable to the SQL Slammer bug when they installed Microsoft Visio.

Two other important applications in a default configuration are Firewall and Antivirus software. Once considered a nice add-on, they now are the central item of almost all corporate computers and many home user systems. The owner used Zone Alarm Pro with Web filtering for his firewall and Norton Antivirus Professional as his Anti-virus solution for this audit. Research on the Internet revealed very little focused documentation for either product.

A search of Norton's web site returned a number of pointed troubleshooting documents but no definitive guide for secure configuration. Zonelab's website yielded the same result. Using Google, I got a lot of general configuration documentation related to Norton's Antivirus Corporate edition but nothing on their end-user product. For Zone Alarm, I found several general configuration guides authored by universities! I also found a user forum bulletin board site where you get answers to pointed questions regarding Zone Alarm. In addition, I referenced Michael Hagerty's SANS contribution on Mobile computing. He has very through sections on Norton Antivirus and Zone Alarm security (33). I also reviewed Martin Naedele's article on Zone Alarm security though it was based on an earlier version with a much different interface (39).

How to handle it?

Microsoft again leads the way in addressing known security issues and those discovered in production use. The key again is user intervention. There are several Microsoft administrative guides and administrative templates available that can be installed through Group Policy manager. They contain numerous settings for securing the application in question. As in the case with the operating system, a balance must be struck between security and ease of use with applications. Many security settings that protect the application might make it more difficult for the user to do their work. An individual consultant may not have an issue with it as he can easily turn settings on and off as he needs them. A small consulting firm will need a balanced consensus for its security settings. Once these setting are decided on they will need to be secured against the employee consultant changing them. Below are some suggestions for accomplishing this:

1. **Patch the application:** Keep up to date through www.Cert.org, SANS, for application vulnerabilities. Go to the vender's website on a regular basis. When there are updates download and apply them.

2. **Apply Security Settings through the MMC/Group Policy Editor and the SCA Snap-ins:** There are a large number of settings that can be applied to all of Microsoft's products.

3. **Disable Automatic Updating:** This is where I differ from mainstream thought. I do not trust the Internet enough to feel comfortable with automatic downloading. It only takes a simple redirect hack of the system or the company server to send the update application to the bad guy's website. It would be better to disable automatic update and enable it or do a manual update when I am going to be there and I'm aware of it so I can oversee it. That is my responsibility as a laptop owner and as a responsible consultant. However, this can be a very individualized option. Again, an independent consultant will feel more comfortable with manual updating than a consulting firm with a larger administrative burden.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. **Review third party applications before installing them:** The current trend in bundled Adware and Spyware with third party applications, freeware and shareware presents a significant risk when looking to use freeware, shareware and small business software. Adware and Spyware sits on one's computer and monitors the use of the computer and its use on the Internet. The software then sends that information back to its originator who can then tailor web or email-based advertising to be served up to the computer's owner. Increasingly this type of software is being used maliciously to steal personal information, account numbers, usernames and passwords. It helps to do a little research of the software to ensure there are no hidden problems and to verify any secure settings that will enhance the software's security profile.

3.4 Network/Internet Risk Analysis

The Internet and, through its connections, the company's or user's network are the primary vectors through which the majority of attacks to computers occur. The primary culprit of these vulnerabilities is the TCP/IP protocol suite. It was originally designed in the 1970s as a communication standard for the emerging ARPANET. TCP/IP proved its worth in the 90s as networking computers together become popular. Due to its popularity and relatively cheap components, it quickly became the de-facto standard for business networks and allowed for transparent connection to the Internet, where it was already the accepted standard. However, many of the shortcomings of the TCP/IP protocol suite became apparent as the Internet caught on in the late 90s.

The key advantages of the TCP/IP suite are its flexibility and its ability to address all seven layers of the Open Systems Interconnect (OSI) model trough translation of it's four layer model. These advantages are also its curse. The many pieces that make up the suite and give it flexibility each also make it vulnerable to exploits.

For example, DNS cache poisoning affects the Domain Name Service protocol. ARP cache-poisoning affects the Address Resolution Protocol. The File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are open to session hijacking. The three-way handshake that is the core of TCP/IP's connection oriented connection established is open to SYN and Denial-of-Service attacks.(31,32)

Spyware is another category of malicious code that uses the Internet as its conduit. Applets and code can be hidden in website pages or downloadable software can be silently installed on the local machine or reside on it as a cookie. At the minimum, the code can be an unwanted application installed without one's permission by an Internet retailer. As you step the scale the software may be unknowingly installed and may track one's Internet browsing or log their keystrokes. This information is then sent back through the Internet to the source. A good example is some research I am doing on Screensavers. Several free, demos and full versions of Screensavers routinely install spyware on the user's machine. In one company's case, they ask for your permission and still install the spyware even after you've clicked no.

A consultant or a small business consulting firm has this risk again magnified by the number and diversity the client networks that he/they connect to. There is no way to rely on the security measures of the host network since there is no way to be sure of the level of security of those networks. For the consultant/firm it falls back to insuring that their laptops are secured. For instance:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. **Harden the TCP/IP stack:** Microsoft and third party articles discuss registry changes that will harden the TCP/IP protocol against Denial of Service type of attacks.

2. **Disable TCP/IP services:** If services such as NETBIOS over TCP/IP, FTP or Telnet are not needed, they should be disabled. If only needed occasionally, they should be set to manual and started only when needed.

3. **Utilize a Personal Firewall:** A personal firewall, correctly configured, can detect and prevent external attacks from the network and the Internet. It also can insure that if somehow compromised by a key logger or Trojan, that only the allowed traffic will be transmitted to the external network.

4. **Utilize an Anti-virus program:** An Antivirus program will detect and protect against infiltration from virus-borne attacks. It provides its protection through an engine, tied to virus definition files that contain behavior signatures that the engine uses to detect and eliminate viruses.

5. **Utilize a Spyware program:** Like an anti-virus program a spyware program uses a definition file to aid in detection and elimination and also looks for Trojans and key loggers. Additionally, a Spyware program looks at cookies, known registry entries and, in some cases, can install entries in the registry to "immunize" the system from further spyware infections.

6. **Encrypt Data Traffic Flows:** Whenever possible, IPSEC VPNS or SSH should be used to encrypt communications to the network or Internet.

II. Create The Audit Checklist

4. The Audit Process

The goal of this section is to define the checklist parameters, create the checklist and perform an audit of a laptop using the checklist. It should be noted that to audit a Windows-based computer and it's myrid number of Operating System and application settings can result in a large scope. The purpose of this checklist is to create a document that addresses a prominent subset of important security settings to a moderate level of granularity at a minimum. It will encompass the laptop, Windows, the common use applications and common security applications into one document. This is a unique from most past audit papers on this subject that tended to hone in on one facet of the system or another. The checklist will also focus on the Microsoft configuration and testing tools.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.1 The Audit Criteria

In creating this checklist the primary tools to be used for checking security are the Windows Security Configuration and Analysis tool the Group Policy tool and the Microsoft Baseline Security Analyzer. The Security Configuration and Analysis tools can help set the baseline security profile for a Windows computer as will as checking that profile against a defined template and automating the update of changes to security settings. The Group Policy Manger tool provides a real-time view and change capability to a major subset of the security settings. Appendix B outlines the basics for setting them up for use in the MMC.

The Microsoft Baseline Security Analyzer checks the primary Windows security elements and performs tests on some of them much like a basic vulnerability scanner. It then outputs a report of what was found.

This audit checklist will cover 6 primary areas. Within each area will be checklist items addressing the specific security settings of that area. The primary source for the majority of the operating system and application settings is the Windows XP Security Guide. Several of the referenced resources are used to address the laptop physical security and network/Internet security.

Some of the settings addressed in these checklist items might appear trivial to some. The role and nature of most laptops and the environment they work precludes that a broad range of security controls be addressed, even when they may be viewed as inconsequential. A good example is a BIOS password. Several guides including the NIST and NSA guides require it as a level one-security setting. To any body with some in depth computer experience this control could be easily bypassed allowing access to the Operating System. And yet, to some thieves with only some or no experience, this item represents a potentially highly effective control. Since the majority of laptop thefts involve thieves are looking to turn a quick profit on the resale of it, a BIOS password has the potential to render their ill gotten gain and it's information useless as profit maker.

The checklist utilizes the primary categories required to meet the control objective. The reference category lists the primary resource(s) cited. Other resources referenced in this document may also address the line item in question. The risk column identifies the risk potential of item and wither this is an objective (yes/no) or subjective (open to interpretation) item. Risk Analysis quantifies the risk.

Testing /compliance addresses each item in two ways. Verification provides the binary component. It is either correctly configured (compliant) or not correctly configured (not compliant). Validation provides the testing component to insure the setting is working as configured. Some objective items may not have or require an associated validation procedure. Likewise some items may have a validation procedure that, at first appears to be not needed. However, in these cases, in order to insure the associated setting reviewed has not been superceded by setting not reviewed a test of the control is required.

4.2 The Audit Checklist

The audit checklist I have created combines several existing standards and guidelines I have referenced into a comprehensive guide that can be used to insure that the laptop of a consultant or a small business consulting firm is secure. I have chosen to use a more checklist-based format than a narrative/checklist-combined format that I have seen others use. The purpose in doing so was to create a more streamlined interface for the end user to utilize. The goal is ease of use.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A person desiring to use this checklist could cut and paste it into a new document in one section, modify it to their needs and begin auditing. As I worked to create this checklist, the sheer number of security settings that could be addressed in the Microsoft components overwhelmed me. To provide a more manageable scope I pared the checklist down to the most important settings across the spectrum of components I chose to evaluate.

There are varying degrees of security configuration depending on whether you are consultant or a consulting business. This is particularly true when it comes to things like application security. For example, Internet Explorer has several very granular settings related to what one can do with access and download of web content. A consulting firm with multiple laptops and consultants and the added risk from connecting to the company network may be inclined to more restriction. An individual consultant may not be as concerned and therefore may opt for the less restrictive settings. I chose to include all security settings I felt were relevant to the system's role.

The risk settings include the level of risk (Low, Medium, High) and whither it is a subjective (S) or an objective (O) evaluation. The Status column indicates a Pass, Fail or Not Applicable (N/A) depending on the importance of a particular line item to a company or consultant and/or wither it is an acceptable risk or not determines it's applicability to the overall grade. Some line items may not be applicable. High-risk items should never be considered as non-applicable. To do so invites compromise of the system. Medium and low risk items could be listed as non-applicable after they are evaluated and agreed upon as acceptable risk.

Grading of pass/fail on a line item is a measurement of how the system meets the objective. For the audit overall, pass/fail is a more subjective measurement. Failure of any high-risk line item should constitute failure of the audit overall. Failure of an accumulation of medium-risk items should constitute failure of the audit. However, which line items failed, whether they were objective or subjective and what a company/consultant feels is an acceptable risk plays a large role in that determination.

For the purposes of my demonstration, audit failure of any one high-risk objective item or three high-risk subjective items constitutes failure. Failure of any 10 medium risk objective items constitutes failure. This is based on personal perspective and experience as an independent consultant. A consulting firm may elect a more stringent baseline for the pass-fail criteria based on the nature of their business.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Laptop ID: _____

Item:	
P= Physical Security	W= Windows Security
U= User Account Security	F= File Security
NI= Network/Internet Security	A= Application Security

Risk = **H**igh **O**bjective
Medium **S**ubjecti ve
Low

Status= **P**ass
Fail
N/A (Not Applicable)

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
P1	Ensure laptop bag is properly identified.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	MO	Proper bag identification will deter theft. Stolen bag can be readily identified.	Some type of identification or ID marking should be viewable	1. Verify the use of marking pen on bag and/or luggage ID tag holder and/or the use of ID Tag(s) or business card(s) in bag compartment(s). Use surface.	
P2	Ensure Laptop bag can be secured.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Personal experience.	LO	Unsecured laptops in public settings are open targets and can be easily stolen when no one is looking or is distracted.	A method to secure the bag must be present and in use	1. Verify the use of cable & lock for bag and luggage lock for laptop compartment.	
P3	Ensure Laptop is properly identified.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. LabMice Laptop Security Guidelines. (Ref 27)	MO	A laptop without unique identification is easier to steal and resell.	Some form of asset marking tag must be present.	1. Verify use of asset tags (Corporate). 2. Verify use of tamper proof ID tags such as STOP tags.	
P4	Ensure laptop can be physically secured when in use.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. LabMice Laptop Security Guidelines. (Ref 27)	HS	41.3% of laptop thefts occur in the workplace	A Laptop locking device must be present and use must be validated	1. Verify the use of cable lock or locking Docking Station. 2. Validate use of security device in the primary work area and check to insure it actually secures the laptop when used..	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
P5	Ensure laptop requires BIOS password before allowing access to the BIOS.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. LabMice Laptop Security Guidelines. (Ref 27)	MO	A thief or hacker could be able to access the BIOS to make changes to or undo security-based changes to the BIOS without password security.	The BIOS must be accessible only through a secure access method.	1. Refer to Attachment E for common BIOS access keys and menu configurations. Normally this will be located in the Security menu tab. 2. Verify that a password is required. 3. Validate by attempting to access the BIOS and look for a password prompt.	
P6	Ensure laptop requires boot password before starting the operating system.	LabMice Laptop Security Guidelines Checklist. (Ref 27)	MO	If a thief can boot the laptop up to the operating system (OS) he has a better chance of hacking the OS security.	The system should not be able to start without a BIOS access control method if available.	1. Refer to Attachment 1 For common BIOS access keys and menu configurations. Normally this will be located in the Security menu tab. 2. Verify that a password is required. 3. Validate by initiating normal boot up. Look for a password prompt before the OS is allowed to start.	
P7	Ensure floppy drive is not listed as bootable device.	LabMice Windows XP Security Checklist. (Ref 28)	MO	Bootable floppies can bypass BIOS and operating system security.	A floppy disk must not be able to boot the system.	1. Refer to appendix E for common BIOS settings Normally this will be located in the Advanced settings or the Boot menu tab. Verify that it is set to disable. 2. Validate by inserting a boot floppy and ensuring that the system does not try to boot from it.	
P8	Ensure CD-Rom is not listed as a bootable device.	LabMice Windows XP Security Checklist. (Ref 28)	MO	Bootable CD-ROMs can bypass BIOS and OS security.	A bootable CD-Rom must not be able to boot the system.	1. Refer to appendix E for common BIOS settings Normally this will be located in the Advanced settings or the Boot menu tab. Verify that it is set to disable. 2. Validate by inserting a bootable CD-Rom and ensuring that the system does not try to boot from it.	
W1	Ensure that all Windows Security Patches are up-to-date.	LabMice Windows XP Security Checklist. (Ref 28)	HO	Windows security is tied to security and maintenance patches to the Operating System and Microsoft applications. An unpatched system is an open target.	All current security patches and all relevant general patches must be installed to insure secure configuration.	1. Select **Start/Programs/../Microsoft Baseline Security Analyzer** 2. Select **Scan a Computer** from the right window then select or type in the laptop NetBIOS name in the **Computer Name** window. 3. Select **Start Scan** button. 4. After completion review findings and note red X (fail) and yellow x (acceptable risk?) items.	
W2	If installed, ensure Internet Information Server Components secured.	SANS Top 20 List, W1. (Ref 38)	MO	Unpatched IIS vulnerabilities remain at the top of the list of exploitable components.	If IIS is in use It must be secured with the latest Microsoft Patches and the Microsoft IIS Lockdown tool.	1. **Select Start/Control Panel/Administrative Tools\Services** 2. Review services for IIS and confirm it is started. 3. Validate in **Microsoft Security Baseline Analyzer/Results Window.** Check the IIS Scan section to see if components were found and if they are vulnerable.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
W3	If installed, are Microsoft SQL Server Components secured.	SANS Top 20 List, W2, W3. (Ref 38)	MO	Unpatched SQL components are vulnerable to malicious code.	IfSQL is in use It must be secured with the latest Microsoft Patches	1. . **Select Start/Control Panel/Administrative Tools\Services** 2. Review services for SQL Server service or MDAC service and verify wither they are running or not . 3. Validate In **Microsoft Security Baseline Security Analyzer.** Check SQL Section to see if components were found and if they are vulnerable. 4. Validate by run Microsoft SQL tools and/or SQL Pinger 2.2 to cross-verify SQL security	
W4	Ensure that infrared port is disabled or the service is set to manual and stopped.	LabMice Laptop Security Checklist. (Ref 27)	LO	Infrared file transfer can occur if line of sig ht with system and system IR port can be established.	The Infrared port will not allow an infrared device to connect.	1. Select **Start/My Computer**. 2. Right click and select properties. Select **Hardware** Tab and Device Manager button. 3. Select **Infrared Devices and IR port device.** Right click and verify that set to **disabled** 4. Validate by attempting an IR connection.	
W5	Ensure that the USB port is disabled.	Personal Experience.	LO	USB ports used could be conduit to system compromise if USB and plug and play are enabled.	The USB port will be disabled and no attempt to connect to the USB port will succeed.	1. Select **Start/My Computer**. 2. Right click and select properties. 3. Select **Hardware** Tab and Device Manager button. 4. Select **Universal Serial Bus Controllers** and **Root Hub** device. 5. Right click and verify set to **disabled.** 6**.** Validate by connecting a USB device to the USB port.	
W6	Ensure that unneeded services are disabled.	LabMice Windows XP Security Guide. (Ref 28)	MS	Unneeded active services and their associated open ports can provide an open conduit to allow access and compromise of the system.	FTP, Telnet, Messenger, Universal Plug and Play, RPC/DCOM, Remote Desktop, Remote Registry and Netbios Sharing are co mmon services that are not regularly needed and must be disabled	1. Select **Start/Control Panel/Administrative Tools/Service.** 2. Review running services. Disable an/or set to manual those services not needed on a regular basis. 3. Use GRC tools to verify Raw sockets, DCOM and NETBIOS SHARING and Plug and Play are turned off. 4. Validate by running a port scanning utility like **NMAP** to view open ports/services and compare to TCP/IP Port list. 5. Review **Microsoft Baseline Security Analyzer** for the status of high-risk services.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
U1	Ensure the Administrator account been renamed.	1. Windows XP Security Guide. (Ref 37). 2. LabMice Windows XP Security Guide. (Ref 28)	MO	Most hackers will attempt to locate the administrator account and crack the password on it since it has the highest access level possible.	The Administrator account should be renamed and have an account name that is not unique and all references to its function deleted in the description.	1. Select **Start/Control Panel/ Administrative Tools/Computer Management/Users and Groups/Users:.** 2. Look for administrator account. If there right lick and select **Properties.** 3. Verify that the **Description** is correctly commented. 4. Select **Member of** and verify that no Groups are installed. 5. Validate in **Security Configuration and Analysis Snap-in/Security Options.**	
U2	Ensure a dummy Administrator account been created.	LabMice Windows XP Security Checklist. (Ref 38)	MO	Most hackers will attempt to locate the administrator account and crack the password on it since it has the highest access level possible.	The account will have the name administrator and the standard reference information in the description. The account will have an extremely complex password and no group memberships.	1. Select **Start/Control Panel/ Administrative Tools/Computer Management/Users and Groups/Users:.** 2. Look for administrator account. if there account membership in the Administrator Group. 3. Insure that the comments block for the correct account does not have a reference to administration. 4. Validate in **Security Configuration and Analysis Snap-in/Security Options.**	
U3	Ensure that only required accounts are listed in MMC.	1. Windows XP Security Guide. (Ref 37).	LO	Unneeded, unused and/or unsecured accounts present an easy avenue for a hacker to gain some level of access to the system.		1. Select **Start/Control Panel/ Administrative Tools/Computer Management/Users and Groups/Users**:. 2. Verify all accounts. All required but unused accounts must be disabled (Example: Guest) **NOTE:** An exception would be "filler" accounts to mislead hackers. 3. If present, right click, select **Properties/ Member of** and verify that no groups are installed.	
U4	Ensure the Guest account has been renamed.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Checklist. (Ref 38)	MO	The Guest account specifically is a security hole that has been exploited repeatedly by hackers.	The Guest account should be renamed and have an account name that is standard and does not give a clue to the account's function and all references to it's function deleted in the description.	1. Select **Start/Control Panel/Administrative Tools/Computer Management/Users and Groups/Users:.** 2. Look for Guest account. If not there look for other accounts. 3. Check their account memberships for the Guest Group insure that the comments block for the correct account has not reference to administration. 4. Validate in **Security Configuration and Analysis Snap-in/Security Options** and **Microsoft Baseline Security Analyzer.**	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
U5	Are client domain accounts set to user permissions on local machine?	Personal experience.	MO	A client user account set on the local machine with administrator access to the local machine is an often-overlooked security hole that could be compromised.	Accounts for accessing client networks should not be members of the local Administrators Group	1. Select **Start/Control Panel/Administrative Tools/Computer Management/Users and Groups/Users:** . 2. Select the account(s) in question and double click to open. 3. Select the **Member of** tab and review the group membership. If required, change membership to be the Users group only.	
U6	Ensure all required accounts have the minimal Group membership set.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Checklist. (Ref 38)	LO	Any account with higher than the minimum required access via group membership is another possible security hole.	The minimum group membership for most user accounts is Authenticated users. Any additional Group memberships should be limited to the minimum necessary. The Administrators group should be assigned to no more than two user accounts.	1. Select **Start/Control Panel/Administrative Tools/Computer Management/Users and Groups/Users:** . 2. Select the account(s) in question and right click, select **Properties/Member of** review the group membership. 3. Verify the group memberships.	
	The following checklist items will be checked from the Security and Configuration Analysis (SCA) MMC snap-in as configured in Appendix B.			N/A		Select **Start/Run/MMC** from the start menu. Refer to appendix C for procedures to preconfigure the MMC to use Security and Configuration Analysis tool and Administrative templates.	
	Run an Analysis of the laptop			Windows is by default insecure and requires an analysis of all settings		Right click on **Security Configuration and Analysis** Object. From the menu select **Analyze this computer.**	
U7	Ensure the current password history meets or exceeds database setting.	Windows XP Security Guide. (Ref 37)	MO	The ability to reuse recent old passwords places user accounts at risk for long term exploit. Especially if the user uses a common pattern in creating passwords.	Password History should be aminimum of 24 passwords	1. Select **Password Policy** object. 2. In the right window review the **Enforce Password History** object for differences between the current settings and the database settings.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
U8	Ensure the current minimum and maximum password age meets or exceeds database settings.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Guide. (Ref 28)	MO	Having the same password heightens compromise and it will be a security hole if not changed periodically.	Minimum Password Age should be 2 days Maximum Password Age should be 42 days	1. Select **Password Policy** object. 2. In the right window review the **Minimum and Maximum password age** objects for differences between the current settings and the database settings.	
U9	Ensure current minimum password length meets or exceeds database setting.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Guide. (Ref 28)	HO	Short passwords are much easier than long passwords to hack.	Minimum Password Length should be 8-12 characters	1. Select **Password Policy** object. 2. In the right window review the **Mimimum password length** object for differences between the current settings and the database settings.	
U10	Ensure that the current password complexity meets or exceeds data base setting.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Guide. (Ref 28)	HO	Simple passwords can be easily compromised by most password cracking tools.	Should be set to enabled. Complex passwords should have 8 or more characters and combine random letters and numbers or special characters	1. Select **Password Policy** object. 2. In the right window review the **Password must meet complexity requirements** object for differences between the current settings and the database settings.	
U11	Ensure that the current account lockout threshold meets or exceeds database setting.	Windows XP Security Guide. (Ref 37)	MO	Hackers can use trial and error continuously on an account to obtain a password without some method of denying repeated failures to login. A Denial of Service attack can be launched to forcibly lock the account out.	Minimum threshold with controls in place (see U9, 10 & 14) should allow 3-5 attempts before locking the account	1. Select **Account Lockout Policy** object. 2. In the right window review the **Account lockout threshold** object for differences between the current settings and the database settings.	
U12	Ensure that the current account lockout duration meets or exceeds database setting.	Windows XP Security Guide. (Ref 37)	MO	A hacker will risk discovery or attempt a Denial of Service (DoS) attack if they know they can access a locked out account after a short period of time.	Minimum time should be set to 30 minutes to thwart password guessing and minimize the unavailability of the account from valid lockouts.	1. Select **Account Lockout Policy** object. 2. In the right window review the **Account lockout duration** object for differences between the current settings and the database settings.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
U13	Ensure that reset account lockout counter meets or exceeds database setting.	Windows XP Security Guide. (Ref 37)	MO	A Denial of Service attack would be highly successful if the account lockout counter could not be reset to allow logon attempts.	Minimum time must be greater than or equal to The lockout duration to ensure the account will be re-available.	1. Select **Account Lockout Policy** object. 2. In the right window review the **Reset account lockout counter** object for differences between the current settings and the database settings.	
U14	Ensure that Audit policy settings meet or exceed database settings.	1. Windows XP Security Guide. (Ref 37) 2. LabMice Windows XP Security Guide. (Ref 28)	MO	Without auditing of certain events most unauthorized access attempts could go undetected.	Audit all events except directory service access and process tracking. Audit Success and Failure except privilege use which should be set to audit failure only.	1. Select **Local Policy/Audit Policy** object. 2. In the right window review all **Audit** objects for differences between the current settings and the database settings.	
U15	Test password and account policy.	SANS Top 20, W7. (Ref 38)	HO	Weak or missing passwords can allow easy compromise and unauthorized access to the system.	Testing will validate the settings for U7 through U 14 and insure they are working as configured	1. Create a test account and attempt to create a non-policy password. 2. Use account to login with improper password to test account lockout policy. 3. Select Start/Control Panel/Administrative Tools/Event Viewer Select security log and validate that security events are logged. 4. Utilize password-cracking tools to try and compromise the user accounts. 5. Check **Microsoft Baseline Security Analyzer** and review password security objects.	
W13	Ensure that **Access this computer from the network** is securely configured.	Windows XP Security Guide. (Ref 37)	LO	Unsecured access from the network would allow guests and anonymous users to connect to this system. An easy access for hackers	The Administrators and the Users groups will be the only groups listed in this setting. The Everyone group must be removed if present	1. Select **Local Policies\User Rights Assignment.** 2. Select the **Access this computer from the network** object. 3. Verify that administrators and users are the only groups listed in Computer Setting.	
W14	Ensure that **Allow log on through Terminal Services** is securely configured.	Windows XP Security Guide. (Ref 37)	MO	Terminal Services is a communications conduit for compromise of the local system.	Terminal Services, if not used, should not have any groups assigned to it. The Everyone Group must not be assigned.	1. Select **Local Policies\User Rights Assignment.** 2. Select the **Allow log on through Terminal Services** object. 3. Verify that no groups are selected in Computer Setting.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
W15	Ensure **Back up files and directories** are securely configured.	Windows XP Security Guide. (Ref 37)	LO	The ability to backup files and folders can be compromised and bypass restrictive file and folder permissions.	The Administrators and Backup Operators are the only groups assigned The everyone Group must not be assigned. Regular users should not be able to backup files.	1. Select **Local Policies\User Rights Assignment.** 2**.** Select the **Back up files and directories** object. 3. Verify that Administrators and Backup Operators are the only groups listed in Computer Setting. 4. Validate by logging in as a user and attemping to back up files (**Start/All Programs/ Accessories /System Tools/Backup**).	
W16	Ensure that **Debug programs** is securely configured.	Windows XP Security Guide. (Ref 37)	LO	The ability to debug programs can be exploited and capture security information.	Unless required by the nature of the work. the ability to debug programs should be disabled.	1. Select **Local Policies\User Rights Assignment.** 2. Select the **Debug programs** object. 3. Verify that no groups are listed in Computer Setting.	
W17	Ensure **Force shutdown from remote system** is securely configured.	Windows XP Security Guide. (Ref 37)	LO	Forcing a remote shutdown can deny services of servers, in particular, to be unavailable to users.	The Administrators group will be the only group assigned to the Force remote shutdown setting.	1. Select **Local Policies\User Rights Assignment.** 2. Select the **Force shutdown from remote system** object. 3. Verify that administrators are the only group listed in Computer Setting.	
W18	Ensure **Log on locally** is securely configured.	Windows XP Security Guide. (Ref 37)	MO	Default configuration allows anyone to login including anonymous users.	The Administrators Group and Authenticated Users Group are the only groups assigned his right. The Everyone Group and Users group must be removed from this setting	1. Select **Local Policies\User Rights Assignment.** 2. Select the **Log on locally** object. 3. Verify that Administrators and Authenticated users are the only groups listed in Computer Setting.	
W19	Ensure **Restrict CD-Rom and Floppy Access** is enabled.	Windows XP Security Guide. (Ref 37)	LO	Floppy and CD-Rom could be used remotely to compromise a system and upload malicious code.	This setting must be enabled to restrict access of the floppy drive and Cd-Rom to locally logged on users.	1**.** Select **Local Polices\Security Options.** 2. Select the objects **Devices: Restrict CD-Rom/Restrict Floppy access to locally logged-on user only.** 3**.** Should be set to enable in Computer Setting.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
W20	Ensure Interactive Logon settings are securely configured.	Windows XP Security Guide. (Ref 37)	MO	Hackers can social engineer or hack domain account naming convention or password information.	The interactive logon settings should be configured to limit access (Ctrl+Alt+Del enabled), Information (do not display user name), warn of Unauthorized access (message text and title). And insure passwords are changed in a timely manner (Password change prompt - 7days)	1. Select **Local Policies/Security Options/ Interactive logon** and verify the following objects in Computer Setting: 2. **Do not display user last name:** Set to enabled. 3. **Do not require CTRL+ALT +DEL:** Set to disabled. 4. **Prompt User to change password before expiration**: Set to 7 days. 5. **Message text and title for users attempting to logon**: Both configured with messages to warn rather than invite users onto the system. 6. Validate by reviewing system login for correct configuration.	
W21	Ensure that communications with SMB Servers are secured.	Windows XP Security Guide. (Ref 37)	MO	Plain text passwords and no Digital signing of packets occurs if these settings are not configured. This could lead to a system compromise.	The SMB communications should be configured to use encrypted digital encryption and not allow unencrypted communication.	1. Select **Local Policy/Security Options/ Network Client** and verify the following objects in Computer Setting: 2. **Digitally sign communications (If server agrees)**: Set to enable. 3. **Send Unencrypted password to 3rd-party SMB servers**: Set to disabled.	
W22	Ensure that Network Access objects are securely configured.	Windows XP Security Guide. (Ref 37)	MO	Anonymous Users can use null session exploits to compromise the local system.	All settings should limit anonymous access to network components and minimize local storage of logon credentials	1. Select **Local Policy/Security Options/ Network Client** and verify the following objects in Computer Setting: 2. **Do not allow anonymous enumeration of SAM accounts (and shares)**: Both set to enabled. 3. **Do not allow storage of credential ot .NET Passports for network authentication**: Set to enable. 4. **Restrict anonymous access to Named Pipes and Shares**: Set to enable.	
W23	Ensure that Network Security objects are securely configured.	1. SANS Top 20 List, W6. Ref 38) 2. Windows XP Security Guide. (Ref 37)	HO	Windows LAN Manager relies on a weak authentication hash to secure passwords. They are easily cracked providing unauthorized access to a system and network.	LanMan hashes should be configured to the most secure encryption possible (NTLMv2 when possible) and not stored.	1. Select **Local Policy/Security Options/ Network Access** and verify the following objects in Computer Setting: 2. **Do not store LAN Manager hash value on next password change**: Set to enabled 3. **LAN Manager Authentication Level**: Set to Send NTLMv2 only 4. Both **Minimum session security for NTLM SSP-based (including RPC) servers**: Set to Require NTLMv2 session security.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
	End of Security and Analysis and Configuration Snap-in.						
W24	Ensure that Screensaver is used and configured to activate after a minimal period of inactivity and to use a password.	LabMice Windows XP Security Guide. (Ref 28)	MO	Most users will neglect to lock their system when they walk away from it. An internal hacker can access the unlocked system. A screensaver without password enabled can still allow system accessed.	Screensaver must be enabled, configured to require password on resume. Minimum idle time to activate the screensaver should be 5 minutes	1. Select **Start/Control Panel/Display.** 2. Select the **Screensaver** tab. 3. Verify the **On resume, password protect** check box is checked. Ensure that time to activate the screensaver is a minimum of 5 minutes. 4. Validate by checking that the screensaver activates within the required time and then press a keyboard key and see if the screen comes up with a login prompt.	
F1	Ensure that all hard drives are using NTFS.	LabMice Laptop Security Guidelines Checklist. (Ref 27)	MO	Drives using other file systems can be compromised.	All hard drives/ partitions must be NTFS	1. Select **Start/My Computer** and select the drive. 2. Right click and select **Properties.** 3. Verify that the File System reads "NTFS". 4. Validate in the **Microsoft Baseline Security Analyzer**.	
F2	Ensure Simple File Sharing is disabled.	1. LabMice Windows XP Security Guide. (Ref 28) 2. SANS Top 20 W4.5. (Ref 38)	MO	A public shared volume or folder without an security set can easily accessed from the network and this could lead to compromise.	Simple File sharing must be disabled	1. Select **Start/My Computer/Tools/Folder Options**. 2. Select **View/Advanced Settings** window **Simple File Sharing** box should be unchecked.	
F3	Ensure that the Everyone group is replaced with Authenticated Users group on all folders/files.	LabMice Windows XP Security Guide. (Ref 28)	MO	The Everyone group allows anyone, authenticated or not, who can gain access to the computer can have access to folders and files	The Everyone Group includes anonymous access and must be removed from all files/folders. The authenticated Users Group is more secure than the Users Groups and should be added to files/folders.	1. Select random folders and files. 2. Right click on the object, select **Properties.** 3. Click on the **Security** tab and verify that the group membership is, at a minimum, Authenticated Users. 4. Double-check the rights for the group. At a minimum read and execute should be checked for most folders and files. Additional permissions should be used only where needed.	
F4	Ensure that the Encrypted File System is applied to the My Documents and Temp folders at a minimum.	1. LabMice Laptop Security Checklist. (Ref 27) 2. LabMice Windows XP Security Checklist. (Ref 28)	HO	Information access theft has a far more severe negative impact then the actual equipment loss The My Documents and temp folders are where most documents and their working temp files are stored.	The Encrypted File System should be applied to data folders and temp folders at a minimum	1. Locate the affected folders in Windows Explorer. 2. Verify that they show up in green. 3. Right click on several folders select **Properties** and Advanced button. 4. Ensure that the **Encrypt contents to secure data** checkbox is checked.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
	All the following settings will be addressed from the Group Policy Editor.					1. **Start/Run/gpedit.msc.** 2. Select **Local Security Policy.**	
W7	Ensure Autoplay is disabled.	Windows XP Security Guide. (Ref 37)	MO	An autorun-capable CD could introduce autorun-enabled malcious code even if the system is secured from unauthorized logon.	Autorun enabled CD-Roms should not be able to run when the system is correctly configured.	1. Select **Administrative Temp lates/System**. 2. Select the **Turn off Autoplay** object. 3. Verify that it is enabled. 4. Validate by inserting an autorun-enabled CD-Rom. No executable should run.	
W8	Ensure that Windows "Run at startup" is securely configured.	Windows XP Security Guide. (Ref 37)	MO	Most Trojans and malware will configure themselves to run at startup to be persistently effective.	The **Do not process run/run once list** settings set to enable to prevent malware from activating themselves. Enable **Run these programs at startup** to manually define te startup list.	1. Select **Administrative Templates/System/Login.** Verify the following. 2. **Do not process the run once list:** Set to enable. 3. **Do not process the run list:** Set to enable. 4. **Run these programs at startup:** Set to enable and validate the programs to run at startup.	
W9	Ensure that Windows Remote Desktop is disabled.	LabMice Windows XP Security Guide. (Ref 28)	MO	Remote Desktop can allow one to take control of a system remotely much like PCAnywhere or VNC and is not highly secure.	Remote Desktop should be configured to not allow connections by remote clients.	1. Select **Administrative Templates/Windows Components/Terminal Services**. 2. Verify the following. 3. **Do not allow new client connections:** Set to enable.	
W10	Ensure that Windows Auto Update feature is disabled.	Personal Experience.	LO	Uncontrolled connections to the internet can create the opportunity for "man in the middle" and spoofing attacks.	Windows Auto Update feature should only be enabled when it can be monitored while in use. Otherwise it should be disabled	1. Select **Administrative Temp lates/System**. Verify the following. 2.. **Windows Automatic Updates:** Set to disabled.	
W11	Ensure that Windows Auto Update is set to notify user before download and install	Personal Experience	LO	Automated downloads could cause system compromise without end user knowledge if the data request had been redirected to a hacker endpoint	If and when used Automated updates should be configured to notify the user before taking any action.	1. Select **Administrative Templates/Windows Components\Windows Update**. Verify the following. 2. Configure Automatic Updates: Set to Enabled 3. **Notify before downloading and notify again before installing**: selected.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
	Microsoft Office						
A1	Ensure that Microsoft Word Macro Security Level is set to a minimum of Medium.	Windows XP Security Guide. (Ref 37)	HO	Macros provide a primary conduit for malicious code to find it's way onto a target system or network.	Microsoft Word Macro security should be set to medium or high to mitigate the automatic execution of Macros.	1. Select **Administrative Templates/Office XP/Security Settings.** 2. Select the **Word: Macro Security object.** 3. Verify it is enabled and the checkbox for Medium or High is selected. 4. Validate by opening a test document with an embedded macro Word should generate a warning message.	
A2	Ensure that Microsoft Word is configured to not trust all installed add-ins and templates.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft Word should be configured to not trust Installed add-ins and templates.	1. Select **Administrative Templates/Office XP/Security Settings.** 2. Select the **Word: Trust access to all installed add-ins and templates** object**.** 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. Word should generate a warning message.	
A3	Ensure that Microsoft Word is configured to not trust Visual Basic Project.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft Word should be configured to not trust Visual Basic Objects to automatically execute.	1**.** Select **Administrative Templates/Office XP/Security Settings.** 2. Select the **Word: Trust access to Visual Basic Project** object**.** 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. Word should generate a warning message.	
A4	Ensure that Microsoft Excel Macro Security Level is set to a minimum of Medium.	Windows XP Security Guide. (Ref 37)	HO	Macros provide a primary conduit for malicious code to find it's way onto a target system or network.	Microsoft Excel Macro security should be set to medium or high to mitigate the automatic execution of Macros.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **Excel: Macro Security** object. 3. Verify it is enabled and the checkbox for Medium or High is selected. 4. Validate by opening a test document with an embedded macro Excel should generate a warning message.	
A5	Ensure that Microsoft Excel is configured to not trust all installed add-ins and templates.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft Excel should be configured to not trust Installed add-ins and templates.	1. Select **Administrative Templates/Office XP/Security Settings.** 2. Select the **Excel: Trust access to Trust all installed add-ins and templates** object**.** 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. Excel should generate a warning message.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
A6	Ensure that Microsoft Excel is configured to not trust Visual Basic Project.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft Excel should be configured to not trust Visual Basic Objects to automatically execute.	1. Select **Administrative Templates/Office XP/Security Settings.** 2. Select the **Excel: Trust access to Visual Basic Project** object**.** 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. Excel should generate a warning message.	
A7	Ensure that Microsoft PowerPoint Macro Security Level is set to a minimum of Medium.	Windows XP Security Guide. (Ref 37)	HO	Macros provide a primary conduit for malicious code to find it's way onto a target system or network.	Microsoft PowerPoint Macro security should be set to medium or high to mitigate the automatic execution of Macros.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **PowerPoint: Macro Security** object. 3. Verify it is enabled and the checkbox for Medium or High is selected. 4. Validate by opening a test document with an embedded macro PowerPoint should generate a warning message.	
A8	Ensure that Microsoft PowerPoint is configured to not trust all installed add-ins and templates.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft PowerPoint should be configured to not trust Installed add-ins and templates.	1. Select **Administrative Templates/Office XP/Security** Settings. 2**.** Select the **PowerPoint: Trust all installed add-ins and templates** object. 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. PowerPoint should generate a warning message.	
A9	Ensure that Microsoft PowerPoint is configured to not trust Visual Basic Project.	Windows XP Security Guide. (Ref 37)	MO	Embedded and unsigned Visual Basic applets can execute malicious code.	Microsoft PowerPoint should be configured to not trust Visual Basic Objects to automatically execute.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **PowerPoint: Trust access to Visual Basic Project** object**.** **3.** Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. PowerPoint should generate a warning message.	
A10	Ensure that Microsoft Publisher Macro Security Level is set to a minimum of Medium.	Windows XP Security Guide. (Ref 37)	HO	Macros provide a primary conduit for malicious code to find it's way onto a target system or network.	Microsoft Publisher Macro security should be set to medium or high to mitigate the automatic execution of Macros.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **Publisher: Macro Security** object. 3. Verify it is enabled and the checkbox for Medium or High is selected. 4. Validate by opening a test document with an embedded macro Publisher should generate a warning message.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
A11	Ensure that Microsoft Publisher is configured to not trust all installed add-ins and templates.	Windows XP Security Guide. (Ref 37)	MO	Macros provide a primary conduit for malicious code to find its way onto a target system or network.	Microsoft Publisher should be configured to not trust Installed add-ins and templates.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **Publisher: Trust all installed add-ins and templates** object. 3. Verify the checkbox for disabled is selected. 4. Validate by opening a test document with an embedded Visual Basic code. Publisher should generate a warning message.	
A11	Ensure that Microsoft Outlook Macro Security Level is set to a minimum of Medium.	Windows XP Security Guide. (Ref 37)	HO	Macros provide a primary conduit for malicious code to find it's way onto a target system or network.	Microsoft Outlook Macro security should be set to medium or high to mitigate the automatic execution of Macros.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **Outlook: Macro Security** object. 3. Verify it is enabled and the checkbox for Medium or High is selected. 4. Validate by opening a test document with an embedded macro Publisher should generate a warning message.	
A12	Ensure that Unsafe ActiveX Initialization is enabled.	Windows XP Security Guide. (Ref 37)	HO	Active X components are another conduit for malicious code to be executed on a target machine.	Active X components should be configured to, at a minimum, to alert the user.	1. Select **Administrative Templates/Office XP/Security** Settings. 2. Select the **Unsafe ActiveX Initialization:** object. 3. Verify it is enabled and the Initialize using control defaults menu item is selected. 4. Validate by opening a test document with an embedded Active X control in Internet Explorer. IE should generate a warning message.	
A13	Ensure that Internet Explorer (IE) Security Zones are securely configured.	Windows XP Security Guide. (Ref 37)	MO	Security Zones control allowed and denied access to websites for Internet Explorer. If not configured, access could be allowed to any site including unauthorized sites. Unconfigured control would allow the settings to be changed by the users.	The ability to configure the IE Security Zones should be disabled to prevent users from reconfiguring them to less secure settings.	1. Select **Administrative Templates/ Windows Components/Internet Explorer/Security Zones objects.** Verify the following. 2. **Use only machines settings:** set to enable. 3. **Do not allow users to change policies:** set to enable. 4. **Do not allow users to add/delete sites:** set to enable. 5. Validate in Internet Explorer **Tools/Internet Options/Security.** Look for disabled custom level, security level sliders (2) and site management settings(s).	

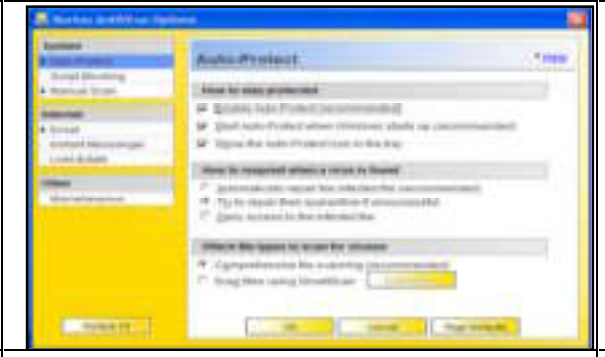
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
A14	Ensure that **Automatic Install of IE components** is securely configured.	Windows XP Security Guide. (Ref 37)	MO	A website that requires the download of a IE component could direct IE to a download site containing disguised malicious code	Install of IE components should be configured not to be automatic.	1. Select **Administrative Templates/ Windows Components/Internet Explorer:** Verify the following**.** 2. **Disable automatic install of IE software components** object**:** set to enable	
A15	Ensure that **Periodic check for IE updates is** disabled.	Windows XP Security Guide. (Ref 37)	MO	The IE Update website could be compromised and a redirect would send IE to a download site containing disguised malicious code	IE Auto Update feature should only be enabled when it can be monitored while in use. Otherwise it should be disabled	**Administrative Templates/Windows Components/Internet Explorer.** Verify the following**.** 1. **Disable Periodic Check for Internet Explorer software updates** object**:** set to enable.	
A16	Ensure that Task Scheduler is securely configured.	Windows XP Security Guide. (Ref 37)	MO	A classic hacking compromise is to install a backdoor and schedule it to run periodically as a task. Security applets scheduled to run periodically could be disabled anonymously	Task Scheduler should be configured to prevent task creation and deletion and can be reconfigured to allow task creation and deletion only when needed.	1. Select **Administrative Templates/Windows Components/Task Scheduler.** Verify the following**.** 2. **Prohibit New Task Creation:** set to enable. 3**. Prohibit Task Deletion:** set to enable. 4. Validate by selecting **Start/All Programs/ Accessories /System Tools/Scheduled Tasks.** Attempt to create a task. If a task is configured attempt to delete it.	
A17	Ensure that Windows Terminal Services is securely configured.	Windows XP Security Guide. (Ref 37)	MO	Windows Terminal Services, when installed, could be compromised and allow access to the local machine.	Windows Terminal services should be configured to require a logon and an encrypted connection the client should not be able to redirect the drive mappings. .	**Administrative Templates/Windows Components/Terminal Services/**	
						/Client Server data redirection: Verify the following**.** 1. **Do not allow drive redirection** object**:** set to enable.	
					Compliance	**/Encryption and Security.** Verify the following**.** 1**. Always prompt client for password on connection** object**:** set to enable. 2. **Set client connection encryption level** object: set to High Level.	

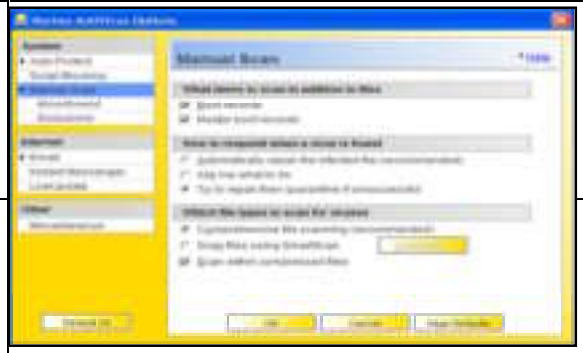
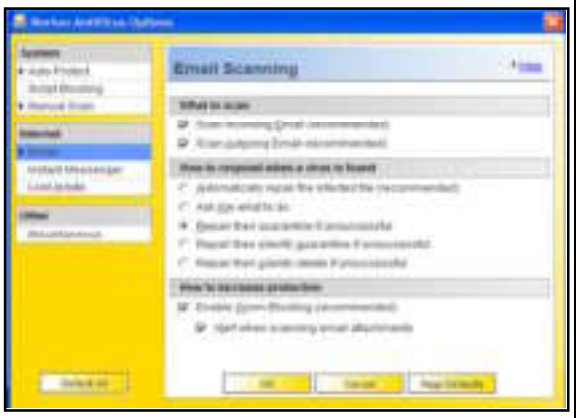
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
A18	Ensure Windows Messenger is not enabled.	Windows XP Security Guide. (Ref 37)	MO	Windows Messenger can be a communications conduit that will allow compromise of the local system.	Windows Messenger should be disabled	1. Select **Administrative Templates/Windows Components/Windows Messenger.** Verify the following. 2**. Do not allow Windows Messenger to be run** object: set to enable.	
	End of Group Policy Editor.						
NI2	Ensure that Internet Connection Sharing is disabled	LabMice Windows XP Security. (Ref 28)	MO	Internet Connection Sharing is a conduit that can give others access to the system and, through It, the network.	Internet Connection sharing should be disabled.	1. Select to **Start/Control Panel/Administrative Tools/Services.** 2**.** Click on **Internet Connection Sharing** and verify that the service is set to **disabled** or **manual**	
NI2	Ensure that Internet Connection Firewall is enabled as needed and configured accordingly.	1. LabMice Laptop Security Checklist. (Ref 27) 2. LabMice Windows XP Security Checklist. (Ref 28)	MO	Uncontrolled traffic in and out of the system can lead to an unobserved compromise of that system	Internet Connection Firewall should be enabled if no other firewall is installed. If another firewall is installed it can be disabled to minimize conflicts	1. Select **Start/Control Panel/ Network Connections**. 2. Select the primary Internet connection. 3. Right click, select **Properties/Advanced** and verify the Internet Connection Firewall checkbox setting. 4. If checked click on settings and verify the Services, Logging and ICMP tabs settings each	
NI3	Ensure Anti-virus Software is Installed.	1. LabMice Laptop Security Checklist. (Ref 27) 2. LabMice Windows XP Security Checklist. (Ref 28) 3. Microsoft Checklist: Using Anti-virus Software (Ref 45)	HO	Viruses represent a significant threat to security.	Anti-virus software must be installed **Compliance**	1. Select **Start/Programs**. 2. Look to see if a Anti-Virus software is installed Norton, McAfee, F-Secure and are some of the more popular brands.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis		Testing/Compliance	Status
	NORTON: Steps						
NI5	Does "**Main Screen Settings**" Match the figure at the right?	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	N/A	All listed objects should be listed in green.		
NI6	Ensure the **Last Full System Scan** was done in the last seven days.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	Infrequently scanned systems can harbor undetected virus infections.	The Last Full System Scan date should be within seven days of the present date.		
NI7	Ensure "**Virus Definitions"** show an last update date with the last 7 days.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	A correctly configure Anti-virus applications can still let viruses in if not updated with the latest virus definition	The Virus Definitions update date should be within seven days of the present date.		
NI8	Ensure "**Options\ System\Autoprotect**" screen matches The figure at right.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	If automated detection and removal is not configured viruses can find their way onto a system hard drive undetected.	Auto-Protect must be enabled and configured to start at Windows startup.		
NI9	Ensure Bloodhound Heuristic Scanning is enabled and configured	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	Risk	Viruses exhibit common behavior characteristics during the course of their work compromising a system.	Bloodhound should be enabled and have the maximum protection possible configured.	1. Select **Scan/Bloodhound** and **Options/Autoprotect/Bloodhound**. 2. Verify the **Enable Bloodhound Heuristics** checkbox is checked. And that the Default level at a minimum is checked.	
NI10	Ensure that Advanced settings is configured correctly	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	Viruses can be introduced by many vectors and at many points in the system startup and operation.	Norton Anti-virus Floppy and removable media scanning, alerting and Windows startup should be enabled.	1. **Options/Autoprotect/Advanced.** 2. Verify that all checkboxes are checked	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
NI11	Ensure that Script Blocking is configured.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)		Macros and Visual Basic scripts can be used to launch viruses, infecting the local system.	Enable Script Blocking and set it to alert to scripts.	1. **Options /System/Script Blocking** has both the **Enable** and the **Ask me what to do…** checkboxes checked.	
NI12	Ensure that **Options /System/Manual Scan** is configured like the figure at right.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	Viruses can insert themselves into numerous places on a system and take many different forms.	Manual Scan should have Boot Records, master Boot Records, Comprehensive, Compressed File as well as Bloodhound scanning enabled.		
NI13	Ensure that **Options /Internet/Email** is configured like the figure at right. Ensure all three check boxes on the advanced tab are checked.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	Email attachments can be carriers of viruses. Spam email can be a nusicence and can generate, intentionally and unintentionally, Denial of Service attacks.	Outgoing email, Ingoing email scanning, Worm blocking, attachment scanning alerting should be e nabled		
NI14	Ensure that Instant Messenger settings are configured correctly.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	Instant Messaging is a conduit through which local system could be compromised.	All Instant messaging scanning and alerting should be enabled even if instant Messaging isn't used.	1. **Options /Internet/Instant Messenger.** 2. Verify that is checkboxes are checked for the all Instant messengers on the laptop.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
NI15	Ensure Antivirus Software can block and quarantine Infected files.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HO	An infected file could be inadvertently accessed if not isolated from normal access, causing virus code to be executed.	The Anti-virus will be tested for its ability to block and/or quarantine infected files, Trojans and email and foe logging the events.	1. Go to www.eicar.org and www.virustest.co.zw 2. Download the virus and email virus test files. 3. The Antivirus software should alert and block the download. 3. Select The Reports tab from the Main screen 4. Review the **Quarantine and Activity/ Threats** reports for virus activity and, If used, **Quarantine activity.** 5. Review the **Activity/Application** Activities report	
NI16	Ensure Firewall Software is installed.	1. LabMice Laptop Security Checklist. (Ref 27) 2. LabMice Windows XP Security Checklist. (Ref 28) 3.Microsoft Checklist: Install a Firewall (Ref 43)	HO	Uncontrolled traffic in and out of the system can lead a unobserved compromise of that system.	All Instant messaging scanning and alerting should be enabled even if instant Messaging isn't used.	1. Select **Start/Programs.** 2**.** Look to see if a firewall software is installed Norton, McAfee, ZoneLabs and BlackIce are some of the more popular brands.	
	Zone Alarm Notes						
N17	Ensure that the **Status** tab of the **Status/ Overview** screen appears similar to the picture to the right.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	N/A	Inbound Protection should indicate attempts having been blocked. Outbound Protection should show programs secured for Internet access. E-mail Protection should show currently active.		

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
N18	On the Main Tab of the Firewall Screen ensure the zones are securely figured.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	Internet access to the computer must be as high as allowable to mitigate scanning and hacking attempts With the Internet Zone set to high The computer is hidden and protected. Selecting medium setting unhides the computer but allows certain file downloading that would otherwise be restricted.	The I**nternet Zon**e is set to High and the **Trusted Zone** is set at least to medium.	1. Select the **Firewall** tab on the left menu ribbon. 2. Select the **Main** tab from the top folder list.	
N19	Ensure that the **Program Control** Screen is securely configured.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	Uncontrolled program access to the Internet can lead to compromise of a system without the owner's knowledge.	The **Program Control** is set to medium at a minimum. **Automatic Internet Lock** ia set to on.	1. Select the **Program Control** tab on the left menu ribbon. 2. Select the **Main** tab from the top folder list. 3. Verify that **Program Control** set to at least medium and **Automatic Internet Lock** is on.	
N20	Ensure that Event Logging is enabled.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	Attempts to compromise the system going through the firewall will go unnoticed without some type of logging enabled.	**Event Logging** must be enabled. **Alert Events** and **Program Logging** must be set to high.	1. Select the **Alerts & Logs** tab on the left menu ribbon. 2. Select the **Main** tab from the top folder list. 3. Verify that the **Alert Events Shown** is set to High **Event Logging** is set to on and that **Program Logging** is set to high. 4. Select **Log Viewer** tab and validate that logs are being created.	
N21	Ensure that Privacy Control is enabled.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	Cookies and spyware ads are known and frequently used vectors to install backdoors and spyware on machines both are also a impediment to Internet browsing.	**Cookie Control** and **AD Blocking** should be set to at least Medium. **Mobile Code Control**, If turned on, should be reviewed and tested for enabled script locking	1. Select the **Privacy** tab on the left menu ribbon. 2. Select the **Main** tab from the top folder list. 3. Verify that the **Cookie Control** and **AD Blocking** sliders are set to at least medium and **Mobile Code Control** is evaluated for use. 4. Validate by browsing websites with Privacy advisor (**Privacy Control/Custom/Cookies)** turned on. Accessing some websites should generate privacy-related Zone Alarm pop-ups.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
NI22	Ensure MailSafe is enabled.	1. Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33) 2. Auditing Zone Alarm (Ref 39)	HO	Email attachments can be carriers of viruses. Spam email can be a nusicence and can generate, intentionally and unintentionally, Denial of Service attacks.	**Inbound** and **Outbound** Protection should be enabled. On the Advanced tab the first two checkboxes (Too many emails, Too many recipients) must be checked and configured for use	1. Select the **E-mail Protection** tab on the left menu ribbon. 2. Select the **Main** tab from the top folder list. 3. Verify that **Inbound MailSafe Protection** and **Outbound MailSafe Protection** are set to on. 4. Validate by sending email(s) with total number of emails and recipients exceeded the parameters in the Advanced tab checkboxes. The firewall should alert and log the activity.	
NI23	Test the Firewall.	Mobile Computing Self-Assessment for Non-technical Business Users. (Ref 33)	HS	A mis-configured or inadequate firewall is a minimal or no deterrent that can be compromised.	Firewall should block and log inbound connection attempts and alert on outbound connection attempts not previously configured.	1. In Internet Explorer, Go to https://grc.com/x/ne.dll?bh0bkyd2 This is their Shields Up!! Firewall test site. 2. Proceed and run Shields Up!! test. The firewall should alert to and log the scan attempt. 3. Use GRC's Leaktest to test a connection going from the computer to the GRC website and it's impact on the firewall. Zone Alarm should alert and log the outbound attempt. 4. In Zone Alarm select the **Logging** tab on the left ribbon menu and check that the alerts were logged.	
NI24	Ensure that some form of Spyware protection is installed.	Personal Experience	HO	Spyware in many forms is anywhere from a nusicence to a high security risk.	Spyware program should be installed.	1. Select **Start/Programs**. 2. Look to see if spyware software is installed. Popular programs include Ad-Aware, Spybot, Spyware Blaster and Spyware Eliminator.	
NI25	Ensure that Spybot Spyware definitions are up-to-date.	Personal Experience	HO	New spyware is being created at an exponential rate.	The most up to date definition file needs to be installed.	1. Check the program's website for current definition file. 2. Verify that the program is using that current file.	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No.	Objective	Reference	Risk	Risk Analysis	Compliance	Testing/Compliance	Status
NI26	Ensure that the _Spybot____Spyware application is blocking and/or finding installed spyware/ cookies	Personal Experience	HO	Spyware has recently become a mainstream issue in regards to system compromise of user information theft.	The spyware application should locate and remove spyware found after a run scan/Browse Internet/rerun scan squence. Most spyware referenced by the spyware software in the IE registry as untrusted should not be found by scanning.	1. Run a spyware check with the software and verify that it locates and eliminates spyware programs it finds. 2. Browse to sites known for spyware 3. Install a software package known to include spyware. 4. Run the spyware software again to check for found spyware.	

End of Checklist

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

III. Audit Evidence

5. Performing The Audit

When I began this practical, I envisioned auditing my own laptop as an administrator. As I got down to getting ready to perform the audit, one of my fellow consultants who was actively consulting offered to let me audit his laptop to perform the audit with. He assured me that he felt that his laptop was fairly well configured for security. I made no changes to his laptop and a couple adjustments to my checklist and began my audit as an outside auditor.

The results of the audit are as a listed as follows. For each area, I have done a short list of the line items audited. Each of the 10 particular items that I chose to describe in detail is included.

5.1 Physical Security

Item	Control Objective	Status
P1	Ensure Laptop Bag is properly identified.	F
P2	Ensure Laptop bag can be secured.	N/A
P3	Ensure Laptop is properly identified.	F
P4	Ensure Laptop can be physically secured when in use.	F
P5	Ensure laptop requires BIOS password before allowing access to the BIOS.	F
P6	Ensure laptop requires boot password before starting the operating system.	N/A
P7	Ensure floppy drive is not listed as bootable device.	N/A
P8	Ensure CD-Rom is not listed as a bootable device.	F

5.2 Windows Security

Item I.

Item	Control Objective	Status
W1	Ensure that all Windows Security Patches are up-to-date.	P

Running Microsoft's Baseline Security Analyzer returned the following Status report for Security Updates (Fig 1) :

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

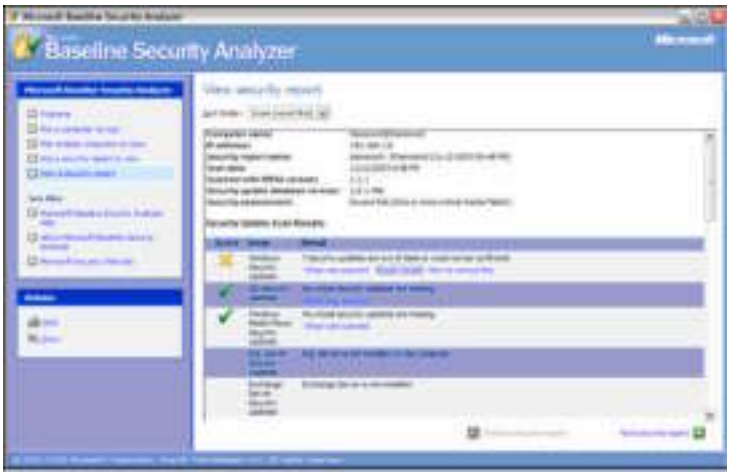


Fig 1



Fig 2

When I reviewed the details of the security updates, the screen above (Fig 2) showed that the updates outlined in yellow were all tagged for file versions that were actually newer than the software expected. Microsoft Security Baseline Analyzer relies on an .xml file in order to analyze the security of Windows. The file, mssecure.xml is a script file with a list of expected settings that are compared to the actual settings. The latest version of this file was released in early in October with the current version of the analyzer. Since then, Microsoft released a whole gambit of patches covering most of their product line. Talking to the owner revealed that he has always been diligent about patching. Some brief research at Microsoft did not yield any answers. As near best as I can conclude, the latest round of patches updated the files in question.

Item	Control Objective	Status
W2	If Installed, ensure Internet Information Server Components are secured.	P
W3	If installed, ensure Microsoft SQL Server Components are secured.	N/A
W4	Ensure that Infrared port is disabled or the service is set to manual and stopped.	N/A
W5	Ensure that the USB port is disabled.	F

Item II.

W6	Ensure that unneeded services are disabled.	P

Reviewing the services applet showed that many security critical, unneeded services were actually disabled. A nice cross-reference is revealed in the Microsoft Baseline Security Analyzer. When viewing the services section, the tool will actually inform you of potentially unnecessary services that are installed and their status (Fig 3). The goal of course is that if it isn't needed, don't leave it installed or running.

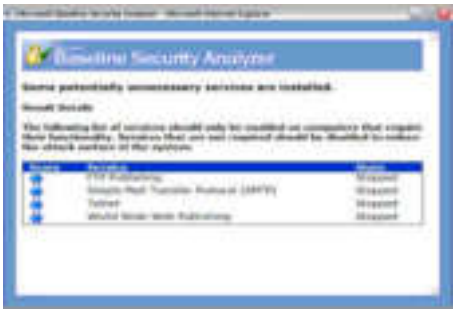


Fig 3

The next test was to run Nmap and determine which ports were open. Almost all open ports can be tied to a running service that is using that port to communicate. I tried a null scan but got No return. The null session settings were securely configured thanks to the configured null session settings. I then tried a SYN

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

scan (nmap -sS -PT -PI -O -T 3). After running the Nmap SYN scan against the system the following ports were found to be open (Fig 4).

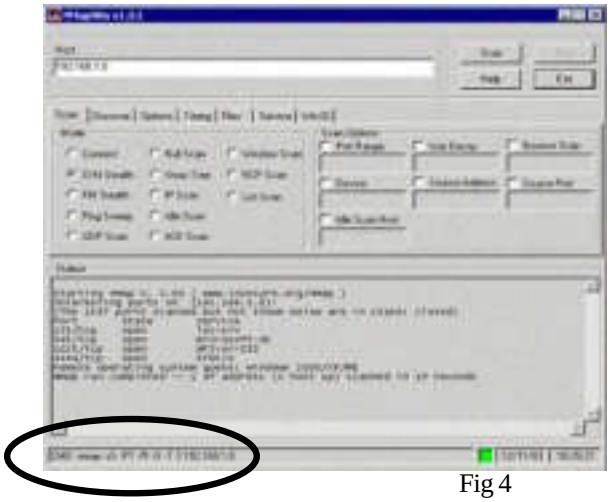


Fig 4



Fig 5

Port 135 is the port associated with Microsoft's well-known DCOM / RPC vulnerability. Running Steve Gibson's DCOMbobulator utility confirmed the vulnerability. Immediate remediation was possible and accomplished (Fig 5). The other open ports belonged to the DS service, IIS and Kerberos. Microsoft Baseline Security Analyzer showed that IIS components were secured. However, it also showed that the IIS lockdown tool had not been run. My conclusion is that this accounts for the open port in question.

Item III.

Item	Control Objective	Status
W7	Ensure Autoplay is disabled	F

Autoplay allows the automatic execution of autorun-enabled CD-Roms. The last Defcon hackers convention had a couple of venders distributing autorun executable CD-Roms configured to install backdoors like Back Orifice on computers. This threat makes the securing of the autorun capability an important security step.

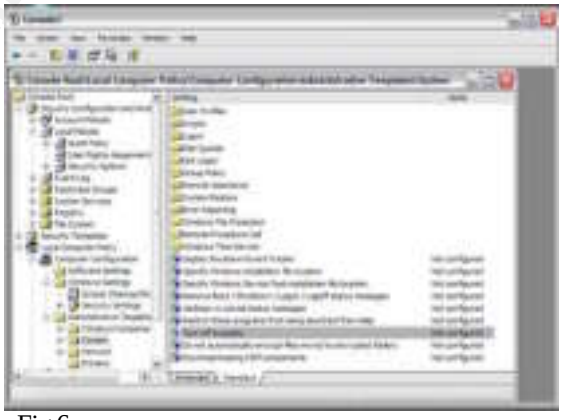


Fig 6

The review of **Group Policy Editor/Administrative Templates/System** revealed that the **Turn off Autoplay** function on this machine was not configured (Fig 6). I confirmed it by inserting an autorun enabled CD-Rom. It immediately presented the menu screen.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item	Control Objective	Status
W8	Ensure that Windows "Run at startup" is securely configured	F
W9	Ensure that Windows Remote Desktop is disabled	F
W10	Ensure that Windows Auto Update feature is disabled	P
W11	Ensure that Windows Auto Update is set to notify user before download and install	F
W13	Ensure that Access this computer from the network is securely configured	F
W14	Ensure that Allow log on through Terminal Services is securely configured.	P
W15	Ensure Back up files and directories are securely configured.	P
W16	Ensure that Debug programs is securely configured	P
W17	Ensure Force shutdown from remote system is securely configured.	P
W18	Ensure Log on locally is securely configured	P
W19	Ensure Restrict CD-Rom and Floppy Access is enabled.	N/A
W20	Ensure Interactive Logon settings are securely configured	F
W21	Ensure that communications with SMB Servers are secured	F
W22	Ensure that Network Access objects are securely configured.	P
W23	Ensure that Network Security objects are securely configured	P

5.3 User Account Security

Item IV.

Item	Control Objective	Status
U1	Ensure the Administrator account been renamed.	F
U4	Ensure the Guest account has been renamed.	F

Looking at the Security Analysis and Configuration tool shows that both accounts have been renamed (Fig 7). However, the names chosen DCH–Admin and Swifty_Guest, I did not feel were generic enough to warrant a passing grade. A hacker could easily pick these accounts out and attack them.

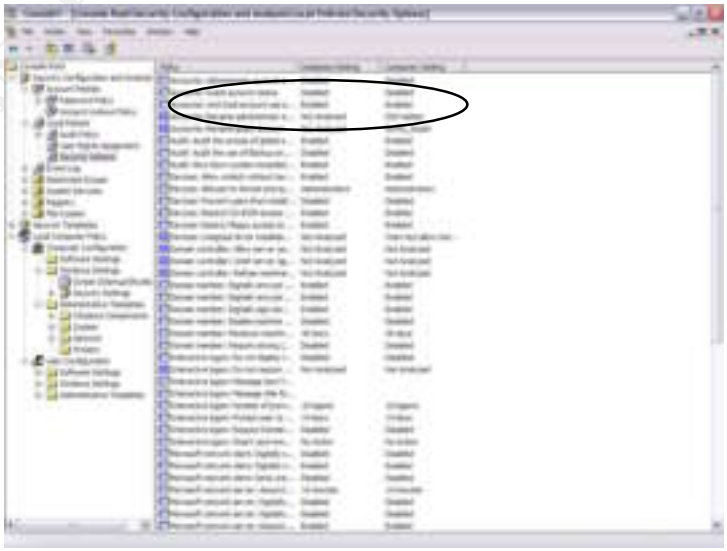


Fig 7

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item	Control Objective	Status
U2	Ensure a dummy Administrator account been created.	P
U3	Ensure that only required accounts are listed in MMC.	F
U5	Ensure client domain accounts set to user permissions on local machine.	N/A
U6	Ensure all required accounts have the minimal Group membership set.	P
U7	Ensure the current password history meets or exceeds database setting.	F
U8	Ensure the current minimum and maximum password age meets or exceeds database settings.	P
U9	Ensure current minimum password length meets or exceeds database setting.	F
U10	Ensure that the current password complexity meets or exceeds data base setting	F
U12	Ensure that the current account lockout duration meets or exceeds database setting.	F
U11	Ensure that the current account lockout threshold meets or exceeds database setting.	F
U13	Ensure that reset account lockout counter meets or exceeds database setting.	F
U14	Ensure that Audit policy settings meet or exceed database settings.	F

Item V

Item	Control Objective	Status
U15	Test password and account policy.	F

Most of the settings for this testing had failed the review portion of the audit. Nonetheless, I decided to move ahead and test what I could. I used L0pht Crack 4 and ran the accounts through it to see how they would fair. As can be seen below (Fig 8,9) two of the accounts, one active and one disabled, did not have passwords. The other two accounts, one active and one disabled, had passwords that were discovered in approximately 15 minutes using brute force. The use of passwords on all accounts and complex passwords combining letters numbers, special characters and length are the cornerstones of good security policy.



Fig 8

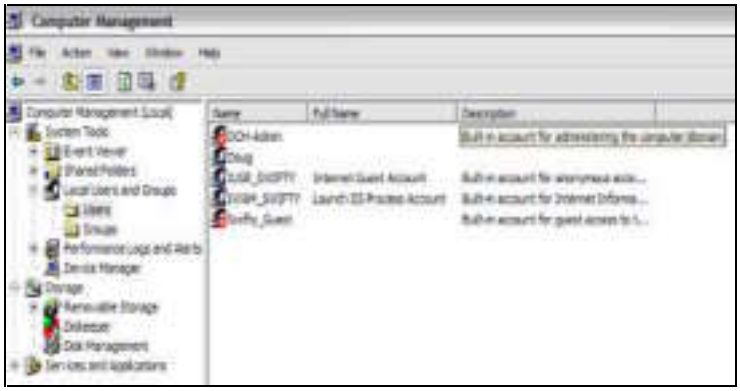


Fig 9

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Next I reviewed Microsoft Baseline Security Analyzer (report view). In contrast to L0phtCrack it showed that all accounts had adequate password settings (Fig 10). It also showed that the system had only two administrator accounts (pass).

Score	Issue	Result
Check passed	Local Account Password Test	No user accounts have blank or simple passwords.

User	Weak Password	Locked Out	Disabled
DCH-Admin	-	-	Disabled
Swifty_Guest	-	-	Disabled
Doug	-	-	-
IUSR_SWIFTY	-	-	-
IWAM_SWIFTY	-	-	-

Fig 10

5.4 File System Security

F1	Ensure that all drives are using the NTFS file System.	P
F2	Ensure Simple File Sharing is disabled.	P
F3	Ensure that the Everyone group is replaced with Authenticated Users group on all folders/files.	F
F4	Ensure that the Encrypted File System is applied to the My Documents and Temp folders at a minimum.	F

Item VI

Item	Control Objective	Status
F5	Validate Group rights to all public shares on the system.	P

I decided to reverse the process on this item in order to expedite the audit. I checked the report that I had run with Microsoft Baseline Security Analyzer. The shares section showed the following (Fig 11):

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

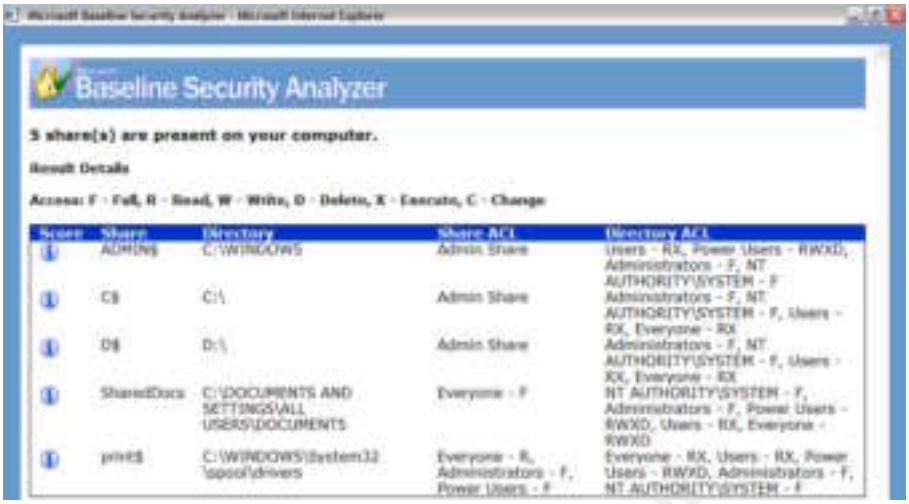
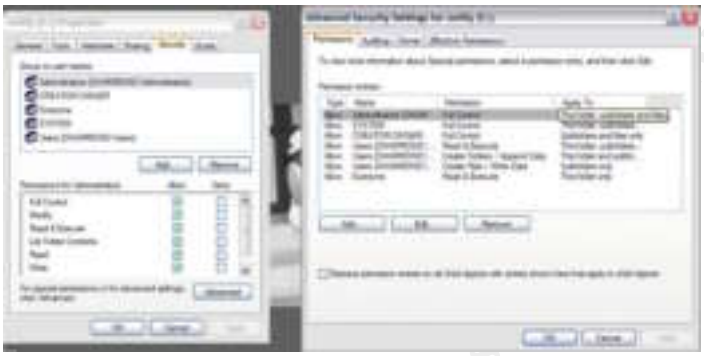
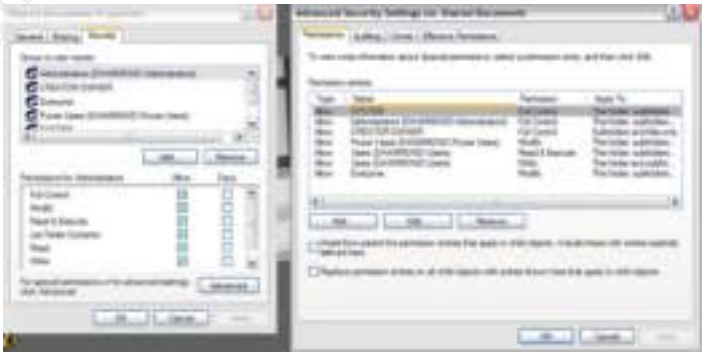


Fig 11

The three admin shares had minimal permissions listed for all groups with only the Admin group and the System Services accounts showing full rights. The two public shares were a little less secure as expected. But, the Everyone group was restricted on the print share to read only which is better than full rights. I verified the findings of the Microsoft Baseline Security Analyzer. The owner did not replace the Everyone group with authenticated users and that was reflected here. I next looked at the shared docs folder and the C$ share and verified the findings of the Microsoft Baseline Security Analyzer (Fig 12,13).


Fig 12


Fig 13

Other than that the overall profile of the shared file system looked pretty secure.

5.5 Application Security

Item	Control Objective	Status
A2	Ensure that Microsoft Word is configured to not trust all installed add-ins and templates.	F
A3	Ensure that Microsoft Word is configured to not trust Visual Basic Project.	F
A5	Ensure that Microsoft Excel is configured to not trust all installed add-ins and templates.	F
A6	Ensure that Microsoft Excel is configured to not trust Visual Basic Project.	F
A8	Ensure that Microsoft PowerPoint is configured to not trust all installed add-ins and templates.	F

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item	Control Objective	Status
A9	Ensure that Microsoft PowerPoint is configured to not trust Visual Basic Project.	F
A10	Ensure that **Microsoft Publisher Macro Security Level** is set to a minimum of Medium.	N/A
A11	Ensure that Microsoft Publisher is configured to not trust all installed add-ins and templates.	N/A
A12	Ensure **Outlook Macro Security Level** is set to a minimum of Medium.	P
A13	Ensure that Unsafe ActiveX Initialization is enabled.	P
A14	Ensure that Security Zones is securely configured.	P
A15	Ensure **That Automatic Install of IE components** is securely configured.	P
A16	Ensure that **Periodic check for IE updates** is disabled.	P
A17	Ensure that Task Scheduler is securely configured.	F
A18	Ensure that Windows Terminal Services is securely configured.	P
A19	Ensure Windows Messenger is not enabled.	P

Item VI

Item	Control Objective	Status
A1	Ensure that **Microsoft Word Macro Security Level** is set to a minimum of Medium.	P
A4	Ensure that **Microsoft Excel Macro Security Level** is set to a minimum of Medium.	P
A7	Ensure that **Microsoft PowerPoint Macro Security Level** is set to a minimum of Medium.	P

A review of the Security Analysis and Configuration tool showed that these three line items were securely configured to Medium level (Fig 14). At this level a document containing an embedded Macro would cause the software to generate a stop/advise warning when attempting to open it. I used a Macro-embedded document in each application and in all three, the warning message popped up when I attempted to open the document. The message for Excel is below (Fig 15).

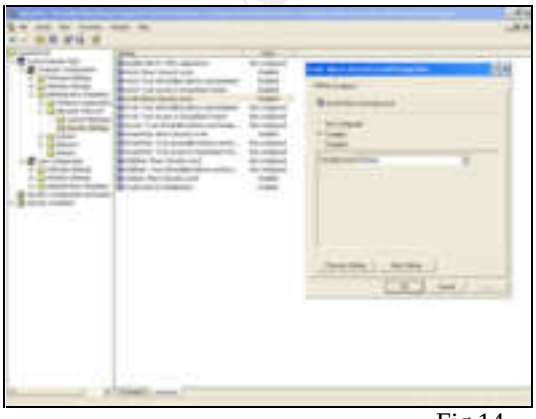


Fig 14

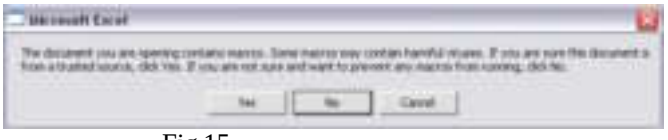


Fig 15

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Microsoft Security Baseline Analyzer confirmed the settings showing that all four installed Office products had secure Macro configurations (Fig 16)

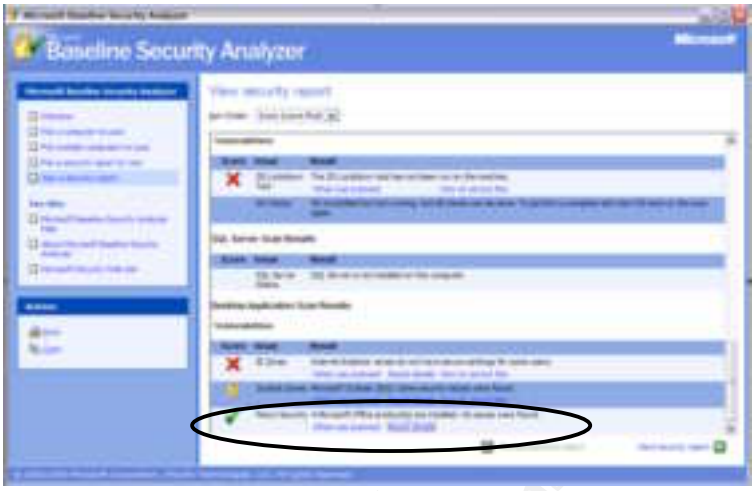


Fig 16

5.6 Network/Internet Security

Item	Control Objective	Status
NI2	Ensure that Internet Connection Sharing is disabled.	P
NI3	Ensure that Internet Connection Firewall is enabled as needed and configured accordingly.	N/A
NI4	Ensure Anti-virus Software is Installed.	P
NI5	Does "**Main Screen Settings**" match the figure.	P
NI6	Was **Last Full System Scan** done in the last seven days?	P
NI7	Ensure "**Virus Definitions"** show an last update date with the last 7 days.	P
NI8	Ensure "**Options\System\Autoprotect**" screen matches the figure	P
NI9	Ensure Bloodhound Heuristic Scanning is configured.	P
NI10	Ensure that Advanced Settings are configured correctly.	P
NI11	Ensure Script Blocking is configured.	P
NI12	Ensure that **Options /System/Manual Scan** is configured like the figure	P
NI13	Ensure that **Options /Internet/Email** is configured like the figure. Ensure all three check boxes on the advanced tab are checked.	P
NI14	Ensure that Instant Messenger settings are configured correctly	P

Item VII, Item VIII.

Item	Control Objective	Status
NI15	Ensure Antivirus Software can block Infected files.	P
NI16	Ensure that Antivirus software can quarantine infected files and log the activity.	P

Antivirus Software is only as good as its ability to block anti virus activity. In order to confirm it you have to attempt to intentionally infect a system. My first test used the procedure described in the checklist. I connected to www.eicar.org. and www.virustest.co.zw and downloaded the virus test files. At the eicar website clicking on the files generated the alert below (Fig19). I next tried the tried the virustest

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

website and requested their test email be sent. When I checked Outlook I found that my ISP had intercepted the emails with their antivirus files. I checked with them only to find out that there was no way they could turn off the antivirus check on my account. I tried Netzero Internet and found that they too strip the attachments off their email.



Fig 17

As an additional test I had on a CD-Rom several pieces of malicious code. I inserted the CD-Rom in the drive and accessed the folder. Norton immediately responded with series of alerts on the various malicious files located on the CD (Fig 21, 22).

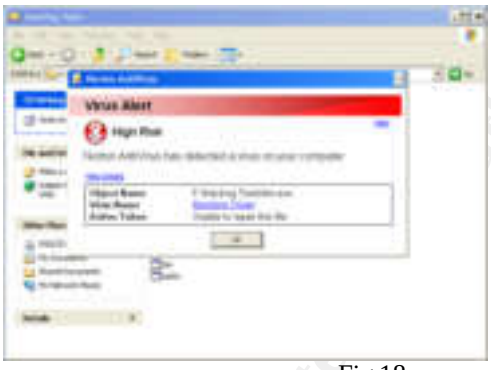


Fig 18

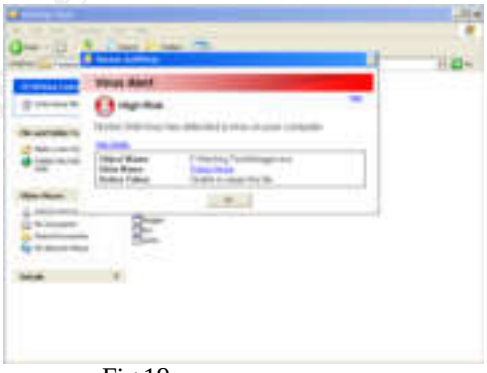


Fig 19

.

I next checked the antivirus logs and found entries for all the tests that I performed.

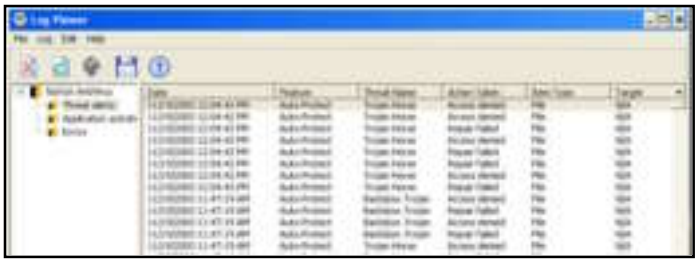


Fig 20

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item	Control Objective	Status
NI17	Ensure Firewall Software is installed (Zone Alarm)	P
NI18	Ensure that the **Status** tab of the Status/ Overview screen appears similar to the picture to the right	P
NI19	On the Main Tab of the Firewall Screen Ensure that the **Internet Zone** is set to **High** and the T**rusted Zone** is set at least to **medium**.	P
NI20	Ensure that the **Program Control** Screen is securely configured	P
NI21	Ensure that Event Logging is enabled	P
NI22	Ensure that Privacy control is enabled	P
NI23	Ensure Mailsafe is enabled	P

Item IX.

Item	Control Objective	Status
NI24	Test the Firewall for vulnerabilities.	P

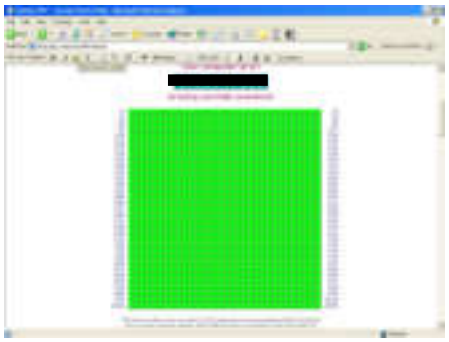
The first test came right out of the procedure. I connected to the Shields Up!! Website and ran the all Service Ports test. Zone Alarm alerted as shown below (Fig 22). After completing the test Shield's Up presented the graphic representation showing Open (red) Closed (blue) and Stealth (green) (Fig 23). I clicked on the text report and it reported that there were no open ports (24).



Fig 21



Fig 22


Fig 23

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Fig 26

Next, I used the GRC Leaktest utility to connect to the Shields UP !! Site. The firewall alerted and blocked the outbound attempt (Fig 25).



Fig 25

Item	Control Objective	Status
NI24	Ensure that some form of Spyware protection is installed.	P
NI25	Ensure that the _Spybot__ Spyware definitions are up-to-date.	P

Item X

Item	Control Objective	Status
NI26	Ensure that the Spybot____Spyware application is blocking and/or finding installed spyware/ cookies	P

Spybot Search & Destroy is the spyware utility that is installed on the consultant's system. Two IT magazines have rated Spybot as one of the better spyware/adware removers in competitive evaluations. In my own experience I found it to be very effective and finding and removing spyware. In addition, it also "immunizes" the system by installing registry entries to Internet Explorer's restricted sites Registry key for a number of IP addresses and websites known to support spyware and adware.

This last feature makes through testing difficult. The target system had had Spybot on it for a while and was thoroughly immunized. That meant that the local machine prevented downloads from most spyware websites.

My initial scan was clean and found no known spyware on the machine (Fig 26). With the permission of the owner I went to the next step. I went ahead and did some Internet browsing. I visited www.gator.com,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

several retail sites that I knew utilized spyware downloads. I then went to www.webshots.com and downloaded and installed their desktop background software. From my personal experience I know the Webshots program installs an adware applet that opens up a backdoor allowing other spyware programs onto the system. I finally installed a couple of screensavers known to install spyware even when you check no. After doing all of this, I ran another scan and Spybot turned up several spy/adware components (Fig 27) and cleaned them off when directed. A follow-up scan returned the same result as the first (Fig 26)

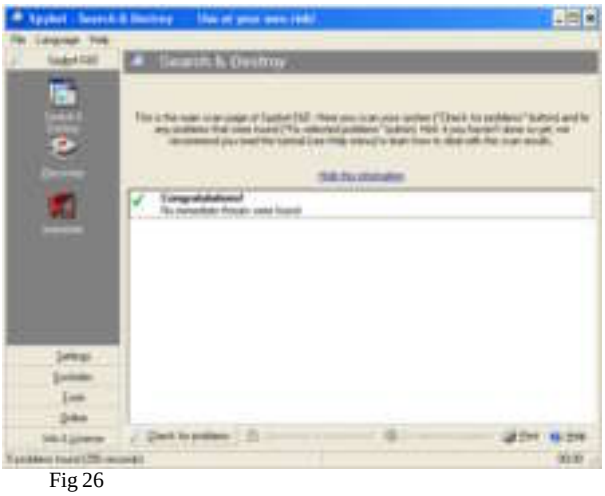


Fig 26

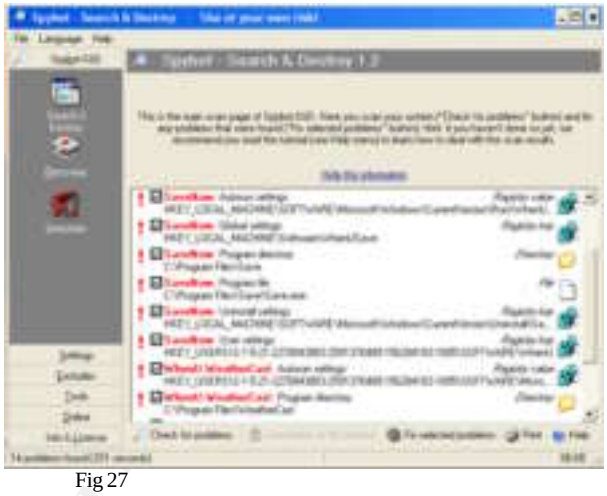


Fig 27

5.7 Conclusions

5.7.1 Security

The goal of security audits is to identify and address risk. Even once an audit is completed and the issues identified there remains residual risk. In the case of the independent consultant that risk is magnified by the nature of the work. Terminal services and Remote desktop in particular offers possible paths to compromise. Most all Control Objectives were addressed in this audit. Those that were not had to do the components not installed or in use on this laptop such as the floppy drive.

This laptop owner has dealt with primary security settings pretty well. He needs to address the less obvious settings that were identified in the audit. It is clear from the number of failed items that he did not address them completely

Physical security was non-existent as a component of the audit. While the owner might be extremely vigilant about surrounding the fact remains that theft or physical compromise is a very prevalent threat and could easily occur at any time. The owner should place identifying tags on his laptop and bag and secure his laptop in use with a security cable. The cost of these controls is minimal (See costs below). The other controls involve BIOS and Boot passwords and removing the CD-Rom from the boot sequence. There is no cost involved here other than time.

Windows Security was fair. Secure settings included Network security Objects and, more importantly, the Services and ports. Insecure settings included the USB port and Run at startup. The important ones were SMB communication and Network Access Objects. Digital encryption on SMB communications is important to mitigate the compromising of user passwords. Configuring Network Access Objects like anonymous enumeration of SAM accounts (and shares) and anonymous access to Named Pipes and Shares:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

securely prevents the use of anonymous null sessions to gather information from the target system. All the failed objectives here could be remediated through settings changes with the only cost being time.

User Account Security was very poor. There were two Administrator accounts. This is not unusual and the Microsoft Baseline Security Analyzer baselines this object at a maximum of two. One account was the primary user account while the other was default Administrator account. However. The attempt to rename the default administrator fell short. The name, DCH-Admin, Made it easy to guess the accounts function. The account was disabled making it harder to compromise. The Guest account too was renamed and disabled. As for the other administrator account it did not have a password and nether did the Internet guest account. The passwords in use were not very strong and were easily cracked. The owner needs to address this area first and foremost. There was no auditing enabled on this system leaving it open to untracked security issues. His laptop is easily accessed and could be compromised without much problem. No direct costs involved here either. Changing the security settings to more secure will only involve time

The File system fared much better. All shares were well secured. Even though the Everyone group was present on shared documents and printers the group's access was limited to Read and execute. I originally failed the Encrypted File System object. The owner informed me after the audit that he normally uses PGP file encryption. This is an checklist improvement issue (see next section). There is little residual risk involved here.

Application Security was another mixed area. The Macro settings mitigated the risk of Macro based malware code. However the ability of Visual basic malware code and trusted add-ins to cause compromise is wide open at the application level. The use of an anti-virus program mitigates this somewhat. IE Security is configured securely. And Task Scheduler appeared to be the only other issue. It is somewhat important to prevent task creation or deletion as a hacker could use it if they gained access to the system.

Network security was the bright spot of the audit as most network settings were configured securely. This is typical of most consultants to concentrate on the obvious perimeter security in deference to internal security. Norton Anti-virus and Zone alarm firewall were well configured to a high level of security. All tests of both passed easily.

5.7.2 The Audit Process

The complete audit of any system like a laptop can become a project onto itself. As the threat grows so does the level of granularity in security settings. Settings that yesterday were of no consequence are today a primary concern. Windows security is made a lot easier with the Group Policy editor and The Security Analysis and Configuration tool, bringing all the myriad settings under one roof in a plain language interface(s). But, it is still the tip of the iceberg.

In reaching the goal of a comprehensive audit of the laptop using the Microsoft tools I feel the audit succeeded. This checklist is a good flexible baseline that can be adapted and expanded for any purpose.

One area of concern for me on this audit was application security. I purposely limited the scope of this area to keep it manageable. Still the checklist needed to address more of the settings in the applications and more applications. The hard part of expanding the application audit portion lies in the volume of applications and lack of security knowledge of many third party applications. So much focus is paced on the many core applications commonly used. There does not appear to be a lot of security research on the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

many third party applications and tools. Vulnerabilities like Nmap's WinPcap library may be out there in some minor application and be unknown.

In discussing the audit with the owner I found another issue that I need to address. The owner did not use EFS to encrypt his data files but he does normally use PGP. In light of that revelation it was clear that I needed to include a line item that addressed alternative encryption technologies other than EFS.

There are some issues with the Microsoft tools. While they appear to be pretty accurate there were still some discrepancies. The incorrect assessment of passwords by the Microsoft Baseline Security Analyzer was one example of their shortcomings. The tools are based on evaluating what is known and cannot assess what is not known. Many tools share this common issue. While not as important in auditing it would be nice if assessment tools could be more proactive and heuristic looking into the possible security issues instead of the known settings.

In using the Microsoft tools I was also concerned about validity. I feel that Microsoft is in the position to best know how to secure their products. This is especially true since their policy of not sharing source code and Application Programming Interfaces (APIs) makes them the primary, bona fide experts. But, could they use this expertise to "cheat" the system? A few years ago video card venders did this. They altered their video card drivers specifically to fool the benchmark software into displaying better performance numbers. Microsoft could do the same thing. In my opinion it would not be above them to do so considering their past. To improve upon my audit in the future I think I will include the use more industry tools as a "cross reference" to insure accurate results.

Finally more thought and work needs to into the evaluation of IIS and SQL. This checklist touched on it but there needs to be more testing of both components. While the Microsoft Baseline Security Analyzer is a good vulnerability scanner It does not appears to any in depth testing of IIS or SQL

IV. Follow-Up

6. Follow-Up of a Consultant Laptop Audit

I have completed the audit of a consultant laptop using the Security Audit Of A Consultant Windows XP Laptop checklist; The overall goal of this audit was determine the level of security utilized on the subject laptop and to address and highlight areas of concern

6.1 Executive Summary

There is no such thing as a totally secure system. In today's dynamic and fast paced world a totally secure system is not a very usable system. The goal of any security audit is to determine the level of security of the audited item and to address any open issues and to increase that level of security. A security audit is also considered a success when it raises the level of security awareness.(33) When it comes to the audit of this system that overall goal is accomplished.

At a more granular level, is the system secure? The goal was not accomplished. Typical of most consultants including myself a lot of attention is paid to the obvious security while attention is not paid to other, less obvious areas. Security issues that are highlighted in industry circles or by the media are the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ones that get the most attention. There is also a level of complacency that tends to insinuate itself into the process. The "it will never happen to me" syndrome causes many to not concern themselves with some security points until they are victimized. That's why auditing is important even for the equipment of IT professionals. It helps to increase their security awareness and brings to light areas of their equipment that they may have overlooked or ignored.

In this case the areas that did well included patching, unneeded services/open ports, network security and macro security The file system security also achieved a passing grade though not directly as I referenced in section 5.7.1

Areas that did not do well included physical security, general Windows security, and application security. My particular concerns were physical and password security. These are areas where I feel that the community as a whole and consultants as a group in particular are very lacking. There needs to be a change both in specific response and in the general complacent attitude towards both physical and password security.

For this audit I highly recommend the use of a security cable, the use of a BIOS password and the removal of the CD-Rom drive from the boot order. Passwords need to be included on all accounts and they need to be strengthened.

The audit itself did not achieve a passing grade. There were to many outstanding issues of medium and high risk that were not in compliance. Each area needs to be reviewed and changes made to bring the security profile up to standard. The consultant uses this laptop on a variety of network environments. By not improving the security of his laptop he places himself and his customers at risk of being compromised and exploited.

6.1.2 Audit Findings

Physical security was completely lacking on the laptop. There were no markings on the laptop bag and no way to differentiate it from other similar bags. The laptop itself had no type of security cable nor identifying tags or markings on it. There was no BIOS password. The CD-Rom was listed as a boot device. This system is an easy target for theft in any situation similar to the two I exampled earlier (18,27). Once out of sight of the owner it would be hard for anyone to identify the laptop or the bag as his. Furthermore, access to the BIOS and/or a simple boot CD could allow the thief easy access to the contents of the laptop.

With Windows security patching of the system was current and up-to date, IIS was disabled as well as most of the unneeded services. Some attention needed to be paid to some of the minor security settings.

There were minimum of user accounts on the system and those not needed were disabled. An attempt to rename Administrator and Guest was accomplished but could be improved. However, both accounts were disabled and that would lesson the attack profile of this portion of the system could be easy to find targets if the system is compromised. An attacker could spend a lot of time trying to hack a disabled account. The Doug account was listed as one of two administrators but did not have a password set for it. It presents an opportunity for a hacker without a password tool to gain access by simply typing the user name and hitting return.

The file system scored well with most shared resources having the proper groups and minimal permissions assigned to each. While the Everyone group had not been replaced with the Authenticated

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Users group the permissions for the everyone group had been set to read or read & execute. While Encrypted File System was not enabled the owner assured me that he normally uses PGP to encrypt his data

Application security was a mixed bag. The Macro security in Office was enabled but Visual Basic was not. While macro enabled Office documents cannot automatically execute, Embedded VBS code in an Office document can be executed. These have long been two major conduits for virus attacks. Active X security controls were also enabled preventing Active X components from executing malicious code.

The Network security was the high point of the audit meeting most all of the objectives. Norton Antivirus, Zonelabs Zone Alarm and Spybot were correctly configured and did their respective jobs well.

6.2 Recommendations

Physical security needs to be addressed. The owner does not travel much outside the local area but his laptop could still be targeted for theft while traveling in the local area and definitely while working at the customer site. I recommend the purchase of a laptop cable for securing the system, and labeling the laptop and the bag. He should also make the changes to the BIOS for the password and CD-Rom boot device.

The owner should also review his user accounts and password security. The naming conventions for his Administrator and Guest account could be stronger. Passwords need to be installed on all accounts and they need to be stronger, more complex passwords.

Finally, the owner should utilize the Microsoft Security Configuration and Analysis tool. He can use the one of the pre-configured templates or select the baseline template and customize the settings to suit his needs. In addition to the settings I have addressed there are additional settings he may want to consider. The Windows XP Security Guide from Microsoft (37) is an excellent reference for these settings.

6.2.1 Compensating Controls

Compensating controls implies short-term solutions to a long-term issue. Most of my recommendations can be implemented immediately as they have minimal business impact. If there would be an issue with implementing them immediately then there are some controls that could be used to mitigate the risk to his laptop. One control might be minimizing the value of the information the laptop has on it. Removing critical business documents or transferring them to removable media and storing it somewhere other than the laptop bag will mitigate the impact if the laptop is stolen. If the correct marking equipment for the bag is not immediately available a Piece of colored cord or string might be used. Again, it won't deter the thief in so much as make the bag identifiable if it is stolen.

6.2.2 Costs

The costs of implementing the solutions are minimal. A good security cable can be purchased for $30 dollars. A luggage tag holder is about $20 dollars. A good "laundry"-marking pen in white for marking the bag is about $10 dollars. Custom asset tags for the laptop cost around $ 20 dollars.

To accomplish the configuration changes to the laptop and it's operating system and to install the above listed solutions would entail a minimum of time on the owner's part. I would estimate 4 to 5 hours at the most

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

with the most of it taken up waiting on Windows to implement some of the changes (EFS) and testing some of solutions. The owner as a consultant would not incur any direct cost for these man-hours. However, this is time he is not available to support his customers. If measured using his base rate of $100 dollars an hour his time to complete these tasks would cost about $500 dollars.

The owner could opt for more expensive solutions but, considering his current and projected routine, the cost may prohibitive. Perhaps the best, most cost effective thing that can be done is simple security awareness. Being conscious of the environment you are in can go along way to insuring that his laptop and contents remain safe and secure.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX A: References

1. "At a Boston hospital, lessons learned from Slammer" Paul Roberts IDG News Service August 14, 2003 http://security.itworld.com/4367/030814hospital/page_1.html

2. " Safeware Loss Chart" Safeware Insurance 2002 http://www.safeware.com/losscharts.htm

3. "2002 CSI/FBI Computer Crime and Security Survey" Computer Security Institute http://www.infragardok.org/files/fbi2003.pdf

4. "2003 CSI/FBI Computer Crime and Security Survey" Computer Security Institute http://www.fdle.state.fl.us/fc3/FBI2002.pdf

5. "FBI Investigating missing State Department laptop" Ann Harrison April 19 2000 http://www.computerworld.com/news/2000/story/0,11280,43904,00.html

6."'Highly Classified' State Department Computer missing" CNN April 17, 2000 Contributions from Associate Press and Reuters. http://cnn.com/2000/US/04/17/state.computer.02/

7. " FBI reports laptops missing" Christopher Dorobek Federal Computer Week July 18, 2001 http://www.fcw.com/fcw/articles/2001/0716/web-fbi-07-18-01.asp

8. "Department of Justice Control over Weapons & Laptop Computers Report No. 02-31" Department of Justice Office of the Inspector General August, 2002 http://www.usdoj.gov/oig/audit/plus/0231/02_31_ED_Plus_Main_Body.pdf

9. "Where the Hell is My Laptop" http://prod.business2.com/articles/mag/0,1640,9294,ff.html

10. "Infosec news reprint of SanDiego Union-Tribune article on Qualcomm laptop theft. Bruce Bigelow Sept 17,2000 http://seclists.org/lists/isn/2000/Sep/0084.html

11. " Stolen Computer Search" Action News 6, Oct14, 2003 http://abclocal.go.com/wpvi/news/101403_nw_computertheft.html

12. "Gone in 6.0 Seconds" Mike Demira Network Computing Sept 30,2002 http://www.networkcomputing.com/1320/1320f4.html?ls=TW_032103_revs

13 "Why is laptop security policy important" Kensington Technology Group http://www.microsaver.com/html/2175.html

14. User Tips/ "Security Statistics" Kensington Technology Group http://www.microsaver.com/html/2178.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

15. SB1386: Senator Peace, Assembly Member Joseph Simitian September 25, 2002
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

16. The Strange Tale of the Denial Of Service Attacks Against GRC.COM Steven Gibson Oct06, 2003
http://grc.com/dos/grcdos.htm

17 "Analysis of MSBLAST.EXE worm" Chris Ream SANs .org
http://isc.sans.org/Analysis_of_MSBLAST.pdf

18. "Teach laptop users these five security musts" Mike Walton Techrepublic April 26, 2002
http://techrepublic.com.com/5100-6255-1043761.html

19." Laptop Computer Security: White Paper, Caveo Technology http://www.caveo.com/images/anti-theft whitepaper.pdf

20. "Unplug n' Pray" history notes Steven Gibson, GRC Corporation http://grc.com/unpnp/unpnp.htm

21." A Brief Summary of My Position on the Denial of Service Windows XP Raw Socket Controversy" Steven Gibson, GRC Corporation http://grc.com/dos/winxp.htm

22. "Microsoft Makes Another Security Pledge" Mike De Maria Oct 30, 2003
http:/www.nwc.com/showitem.jhtml?articleID=15600072

23. "Laptop Security, Part One: Preventing Laptop Theft" Josh Ryder Security Focus July 30, 2001
http://www.securityfocus.com/infocus/1186

24. "Laptop Security, Part Two: Preventing Information Loss" Josh Ryder Security Focus August 13, 2001
http://www.securityfocus.com/infocus/1187

25. Security tip No.8 – Know these laptop security essentials AON Risk Management
http://www.aon.com/risk_management/information_security/security_tip_eight.jsp

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

27. "Laptop Security Guidelines" LapMice.net September 8, 2003
http://www.labmice.net/articles/laptopsecurity.htm

28. "Windows XP Security Checklist" LabMice.net September 5, 2003
http://www.labmice.net/articles/winxpsecuritychecklist.htm

29. "HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000" Microsoft Corporation http://support.microsoft.com/default.aspx?scid=kb;en-us;315669

30. "Encrypting File System Primer: Basics and Best Practices" Kayron Valentine SANS Institute Reading Room Jan 6, 2001 http://www.sans.org/rr/paper.php?id=202

31. "TCP Security" Chris Chambers, Justin Dlolske, Jayaraman Iyer Department of Computer Information Security, Ohio State University
http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

32. “A Topological Characterization of TCP/IP” Giovanni Vigna NEC Research Institute CiteSeer 2002 http://citseer.nj.nec.com/vigna96topological.html

33. “Mobile Computing Self-Assessment for Non-technical Business Users” Michael Hagerty GIAC Practical May 29, 2004 http://www.giac.com/practical/Michael_Hagerty_GSNA_2.doc

34. “Methodology for Auditing The Microsoft Windows XP Operating System” Tony Howlett GIAC Practical Dec 19, 2001 http://www.giac..com/practical/Tony_Howlett_GSNA.zip

35. “NSA Windows XP Security Guide” National Security Agency http://www.nsa.gov/snac/winxp/index.html

36. “What’s New in Security for Windows XP Professional and Windows XP Home Edition Microsoft Corporation July, 2001 http://www.microsoft.com/technet/prodetechnol/winxppro/evaluate/xpsec.asp

37. “Windows XP Security Guide” Microsoft Solutions for Security, Microsoft Corporation

38. “SANs Top 20 Vulnerabilities” SANS.org Oct 8,2003 www.sans.org/top20/

39. “Auditing ZoneAlarm” Martin Naedele SANS.org July, 2001 http://www.giac.com/practical/Matrin_Naedele_GSNA.zip

40. “How to take control of your security settings security settings”, Microsoft Corporation November 24, 2003 http://www.microsoft.com/security/articles/settings.asp

41. “How to maintain your computer for better security ” -, Microsoft Corporation November 24, 2003 http://www.microsoft.com/security/articles/maintenance.asp

42. “Checklist: How to create stronger passwords”, Microsoft Corporation http://www.microsoft.com/security/articles/password.asp

43. “Checklist: Install a firewall to protect your computer”, Microsoft Corporation November 24, 2003 http://www.microsoft.com/security/articles/firewall.asp

44. “Protect your PC, three steps to ensure your PC is protected”, Microsoft Corporation September 9, 2003 http://www.microsoft.com/security/articles/update.asp

Laptop Computer Security White Paper” Caveo Technology March, 2003 http://www.caveo.com/images/Caveo.Laptop%20Computer%20Security.Whitepaper.pdf

47. "Microsoft Baseline Security Analyzer," Microsoft Corporation, http://www.microsoft.com/technet/security/tools/mbsahome.asp

48. “Anti-Virus test file,” eicar online, http://www.eicar.org/anti_virus_test_file.htm

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

50. “ShieldsUP!,” Gibson Research Corporation, https://grc.com/x/ne.dll?bh0bkyd2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX B: Configuring and Using Microsoft Security Analysis and Configuration Tool:

Microsoft , with their release of Windows 2000 and Windows XP, released some new tools to aid in configuration and management of the system in general and security of particular. They include the Group Policy Editor and the Security Configuration and Analysis Tool. This section deals with setting up both snap-ins to run from the MMC and configuring the Security Analysis and Configuration tool to use with your audit

To install these snap-ins You must perform the following steps:

1. Select **start/run** and type in MMC click **OK**.
2. In the MMC select **File/Add/Remove Snap-in.**



Fig 28

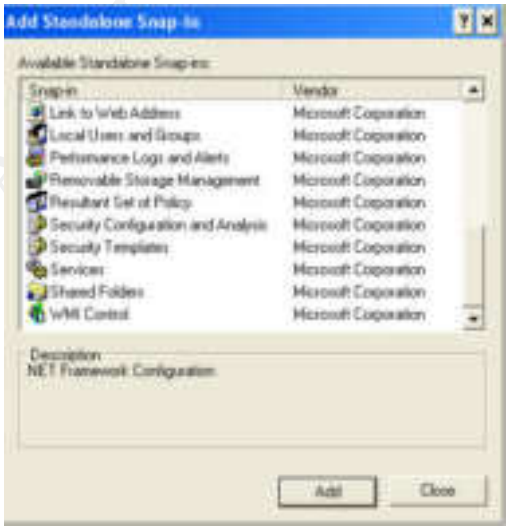


Fig 29

3. Click **Add** and from the list. Select **Group Policy, Security Analysis and Configuration and Security Templates** from the list (Fig 29). NOTE: Selecting group Policy will bring up a wizard for defining the computer(s). Ensure it says Local Computer and click on Finish.
4. After selecting the snap-ins click on OK

When you first use the Security Analysis and Configuration Snap-in you will be presented with another wizard that will ask you to configure a database. You need to configure a baseline security profile (database) in order to utilize the tool to evaluate your security. To configure a baseline database do the following:

1. Follow the instructions in the right pane for creating a new database.

2. The wizard will open up the security templates snap-in . The listed templates are standardized settings for various roles and security levels of Windows.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Select the **security setup** template.

4. Click OK and you are now presented with several objects like below (Fig 30)

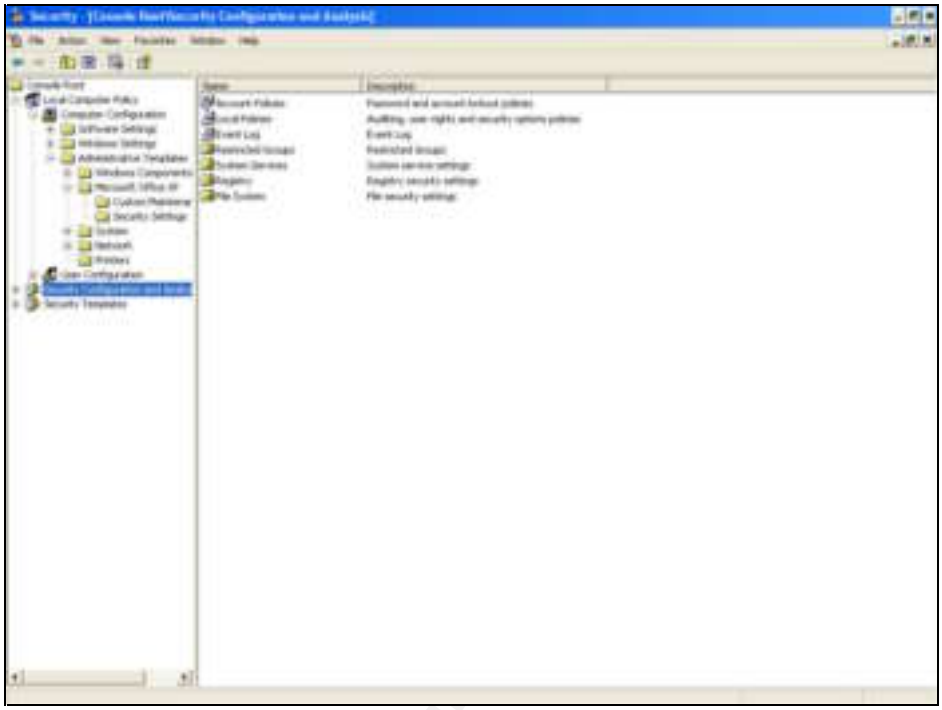


Fig 30

The Security Setup template is some default minimal security settings which are a good baseline to start from You now may want to go through the objects and configure each to suit your needs. As an individual consultant the configuration will be more flexible than a small consulting business. Here, risk to the company network and a desire for more control over how company laptops are being used could lead to more restrictive security settings to mitigate that risk.

Once configured you can right click on the snap-in and select **Configure your Computer** and the changes you have selected will be applied. You are now ready to use the Security Analysis and Configuration tool to analyze your security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX C: TCP/IP ports

The Internet Assigned Numbers Authority (IANA), In conjunction with Request For Comments (RFC), controls and maintains the TCP/IP port database.

0	68 - bootpd/dhcp	156	517 - talk
1 - tcpmux	69 - TFTP)	161- SNMP	520 - RIP
3	70 - Gopher	175 - vmnet	
4	79 - finger	177- XDMCP	521 - RIPng
5 - rje	80 - www-http	178 - NextStep Window Server	522 - ULS
7 - echo	87	179 - BGP	531 - IRC
9 - discard	88 - Kerberos, WWW	180 - SLmail admin	543 - KLogin, AppleShare over IP
11 - systat	95 - supdup	199 - smux	545 - QuickTime
13 - daytime	96 - DIXIE	210 - Z39.50	548 - AFP
15 - netstat	98- linuxconf	213	554 - Real Time Streaming Protocol
17 - qotd	101 - HOSTNAME	218 - MPP	555 - phAse Zero
18 - send/rwp	102 - ISO, X.400, ITOT	220 - IMAP3	563- NNTP over SSL
19 - chargen	105- cso	256	575 - VEMMI
20 - ftp-data	106- poppassd	257	581 - Bundle Discovery Protocol
21 - ftp	109- POP2	258	593 - MS-RPC
22- ssh, pcAnywhere	110 - POP3	259 - ESRO	608- SIFT/UFT
23 - Telnet	111- Sun RPC Portmapper	264 - FW1_topo	626- Apple ASIA
25- SMTP	113 - identd/auth	311 - Apple WebAdmin	631- IPP
27- ETRN	115 - sftp	350 - MATIP type A	632 - mountd
29 -msg-icp	116	351- MATIP type B	636 - sldap
31 - msg-auth	117 - uucp	360	642 - EMSD
33 - dsp	118	363 - RSVP tunnel	648 - RRP)
37 - time	119 - NNTP	366 - ODMR	655 - tinc
38 - RAP	120 - CFDP	371	660 - Apple MacOS
39- rlp	123- NTP	387 - AURP	666 - Doom
40	124 - SecureID	389 - LDAP	674 - ACAP
41	129 - PWDGEN	407 - Timbuktu	687 - AppleShare IP Registry
42 - nameserv, WINS	133 - statsrv	427	700 - buddyphone
43 - whois, nickname	135 - loc-srv/epmap	434 - Mobile IP	705 - AgentX for SNMP
49 - TACACS	137 - netbios-ns	443 - ssl	901 - swat, realsecure
50 - RMCP, re-mail-ck	138 - netbios-dgm (UDP)	444 - snpp, Simple Network Paging Protocol	993 - s-imap
53 - DNS	139 - NetBIOS	445 - SMB	995 - s-pop
57 - MTP	143 - IMAP	458 - QuickTime TV/Conferencing	999
59 - NFILE	144 - NewS	468 - Photuris	1024
63 - whois++	150	475	1025
66 - sql*net	152 - BFTP	500 - ISAKMP, pluto	1050
67 - bootps	153 - SGMP	511	1062 - Veracity

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TCP/IP Ports

1025	1645 - RADIUS Authentication	2301 - Compaq Insight Management Web Agents	4333 - mSQL
1050	1646 - RADIUS Accounting	2327 - Netscape Conference	4444
1062 - Veracity	1680 - Carbon Copy	2336 - Apple UG Control	4701
1080 - SOCKS	1701 - L2TP/LSF	2345	4827 - HTCP
1085 - WebObjects	1717 - Convoy	2427 - MGCP gateway	5000
1100	1720 - H.323/Q.931	2504 - WLBS	5001
1105	1723 - PPTP control port	2535 - MADCAP	5002
1114	1731	2543 - sip	5004 - RTP
1227 - DNS2Go	1755 - Windows Media .asf	2565	5005 - RTP
1234	1758 - TFTP multicast	2592 - netrek	5010 - Yahoo! Messenger
1243 - SubSeven	1761	2727 - MGCP call agent	5050
1338 - Millennium Worm	1762	2766	5060 - SIP
1352 - Lotus Notes	1808	2628 - DICT	5135
1381 - Apple Network License Manager	1812 - RADIUS server	2998 - ISS Real Secure Console Service Port	5150
1417 - Timbuktu	1813 - RADIUS accounting	3000 - Firstclass	5190 - AIM
1418 - Timbuktu	1818 - ETFTP	3001	5222
1419 - Timbuktu	1968	3031 - Apple AgentVU	5353
1420	1973 - DLSw DCAP/DRAP	3052	5400
1433 - Microsoft SQL Server	1975	3128 - squid	5500 - securid
1434 - Microsoft SQL Monitor	1978	3130 - ICP	5501 - securidprop
1477	1979	3150 - DeepThroat	5300
1478	1985 - HSRP	3264 - ccmail	5423 - Apple VirtualUser
1490	1999 - Cisco AUTH	3283 - Apple NetAssitant	5555
1494 - Citrix ICA Protocol	2000	3288- COPS	5556
1498	2001 - glimpse	3305 - ODETTE	5631 - PCAnywhere data
1500	2005	3306 - mySQL	5632 - PCAnywhere
1503 - T.120	2010	3352	5678
1521- Oracle SQL	2023	3389 - RDP Protocol (Terminal Server)	5800 - VNC
1522	2048	3520	5801 - VNC
1524	2049 - NFS	3521 - netrek	5900 - VNC
1525 - prospero	2064 - distributed.net	3879	5901 - VNC
1526 - prospero	2065 - DLSw	4000 - icq, command-n-conquer	5843
1527 - tlisrv	2066 - DLSw	4045	6000 - X Windows
1529	2080	4144	6112 - BattleNet
1547	2106 - MZAP	4242	6050
1604 - Citrix ICA, MS Terminal Server	2140 - DeepThroat	4321 - rwhois	6499

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TCP/IP Ports

6500	9000	27910	32776 - rpc.spray
6502 - Netscape Conference	9090	27960 - QuakeIII	32779 - rpc.cmsd
6547	9200	28000	38036 - timestep
6548	9704	28001	
6549	9669	28002	
6666	9876	28003	
6667 - IRC	9989	28004	
6670 - VocalTec Internet Phone, DeepThroat	10008 - cheese worm	28005	
6699 - napster	10752	28006	
6776 - Sub7	12345	28007	
6968	11371 - PGP 5 Keyserver	28008	
6969	12346	30029 - AOL Admin	
6970 - RTP	13000	30100	
6971	13223 - PowWow	30101	
7000	13224 - PowWow	30102	
7007 - MSBD, Windows Media encoder	14000	30103	
7070 - RealServer/QuickTime	14237 - Palm	30303	
7161	14238 - Palm	30464	
7323	14690	31335	
7777	16969	31337 - Back Orifice	
7778 - Unreal	18888 - LiquidAudio	32000	
7640	21157 - Activision	32771	
7648 - CU-SeeMe	22555	32777 - rpc.walld	
7649 - CU-SeeMe	22703	34555	
7654	22793	40193 - Novell	
8000	23213 - PowWow	41524 - arcserve discovery	
8002	23214 - PowWow	45000- Cisco NetRanger postofficed	
8010 - WinGate 2.1	23456 - EvilFTP	50505	
8080 - HTTP	26000 - Quake	52901	
8100	27000	54321	
8181- HTTP	27001 - QuakeWorld	61000	
8383 - IMail WWW	27010 - Half-Life	65301	
8765	27015 - Half-Life	Multicasthidden	
8875 - napster	27374	ICMP Typehidden	
8888 - napster	27444	9998	
8890	27665	32773 - rpc.ttdbserverd	

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX C: Windows XP Security Features

Kerberos 5 Support: Introduced in Windows 2000, XP includes full support for Kerberos 5. Kerberos was an authentication and authorization system developed by MIT.

Smart Card Support: This feature allows the use of smart token cards with Single Sign On to enhance the security level of user logon.

Support for IPSEC: Introduced in Windows 2000, the use of IPSEC allows securing of communications using 128 bit encryption and VPNS.

Internet Connection Firewall (ICF): A basic firewall ICF is included to provide another layer of protection against network and Internet intrusion. ICF has limited customization capability and is either on or off.

Local Security Policy: Introduced in Windows 2000. Expanded support in Windows XP allows more granular control of the local machine environment.

Software Restriction Policies: Defined in Group Policy in a domain environment, this feature allowed administrators to control what software would be allowed to execute. This allows some control over malicious code

Privacy: New features implemented in Internet Explorer allow more granular control over the management of Internet cookies received by the browser.

Internet Connection Sharing (ICS): A potential security hole, ICS allows one computer with an Internet connection to share it with other computers.

Credential Management: Credential prompting, stored user names/passwords, and the key ring are three new credential management features that enable XP to support Single Sign On.

Improved Certificate Services: XP includes additional administrative features for using digital certificates. They allow administrators in the domain to better control use and renewal of digital certificates.

Encrypted File System (EFS): Another feature introduced in Windows 2000, EFS allowed data files to be secured using 128 bit encryption. Expanded features in XP included multi-user access to encrypted files and encryption of offline folders.

Blank Password Restrictions: XP limits how blank passwords can be used.

Group Security Policy: Using Group Policy Editor in a domain environment network administrators can now apply security settings to multiple users using Group Policy Objects.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Remote Access Control: This feature allows users and administrators to control remote access to the system.

Remote Assistance/Remote Desktop: More of a convenience feature for system support than a security feature, these features are included because of the security risk they represent. Remote Assistance allows administrators a remote control connection to the users machine while Remote Desktop uses Windows Terminal Services to do much the same thing. They both rely on an open port when listening on the network.

Service Context Accounts: Two new service accounts Local Service and Network Service are added to Windows XP. Theses local user security level accounts are meant to replace the local system account that used to be used to run services on the local machine. These accounts mitigated possible network compromise when a local machine service was compromised.

Null Session Settings: New, more granular settings further restrict the use of null sessions to compromise and gather information from target systems.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix D: Common BIOS Security Settings

Most all BIOS have common settings for configuring the system. To that end many of them have unique seings and unique interfaces to common settings. Below are a couple of examples of BIOS with regards to the security settings.

Figure B reprsents the Award BIOS. The Supervisor and the User passwords can be set from the main menu. A Security Setting in the BIOS Advanced features menu controls the use of the passwords through three settings None, System and Setup. System controls Boot access to the system. The Setup setting controls access to the BIOS setup program. The Supervisor password controls BIOS and Boot access while the User password only allows Boot access.

	Setting	Description
Security Option	System	Each time the system is booted, the password prompt appears.
	Setup	If a password is set, the password prompt only appears when you attempt to enter the BIOS Setup program.

Fig A.



Fig B.

Figure C is a different version of the Award BIOS. Here the Set Password function controls the password for both BIOS and Boot access. Again a Security Setting in the BIOS Advanced Feature menu controls how the password is applied, BIOS, Boot or both.

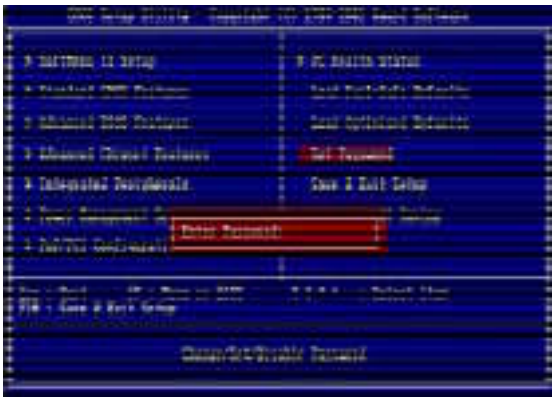


Fig C.

Figure D and E show a version of the AMI BIOS. Here, a dedicated Security tab is where the Supervisor and User password functions are located. Like the Award BIOS the Supervisor password controls boh BIOS and Boot access and the User password only controls the Boot access. Once set, No additional configuration of the BIOS is required





© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.