Global Information Assurance Certification Paper

Securing Window 9x

By
David Groomes

Assignment Version 1.4b opt 1

Abstract

I am going to discuss Securing Windows 95/98/ME computers for home and small business use. Topics I will cover are, why try to secure Windows 99/98/ME. What does a secure computer look like. What available tools are there for accomplishing the task of securing a windows 95/98/ME computer? What are the various user responsibilities? In writing this paper I am going to show how an inherently vulnerable computer, with the installation of 3rd party software, can be made more capable of existing in a hostile environment with significantly reduced risk of compromise.

Why try to secure windows 9x.

Windows 95/98/Me computers were designed by Microsoft to satisfy the evolving needs of computer users. During the time period of windows 95 development, it is obvious that Microsoft was of two opinions, home users and business users. The average home user played games or kept a small about of personal information on their computers and they wanted to be able to run software that ran on their old windows 3.xx or dos.x computers so windows 95 was the answer. Because of using the computer in this manner security was not a consideration in its design. The business or technical user on the other hand wanted to run their existing software that ran on older machines too, but they also want to be able to connect their computers together forming networks to facility the exchange of information and windows NT was the answer here. This leads me to the question why try to secure windows 9x computers when there are alternative operating systems such as Unix, winnt4, win2000, winxp, and other operating systems that have security features already built in. The answer is simple, there are a large number of windows 9x computers connected to the internet. The trouble with Microsoft's two pronged approach was the NT was a little late in coming out and much more expensive, prompting many small business users as well as home users to buy windows 95 computers.

By using information from various locations a rough estimate of the numbers of windows 95/98/ME computers on line can be determined. A poll of 198 users by Mister poll asked business users the question "Which of the following operating systems are used on individual desktops in your organization?" with available choices of operating systems being

Windows XP	Windows 2000	Windows NT 4.x
Windows NT 3.x	Windows ME	Windows 98
Windows 95	Windows for Workgroups	Windows 3.x
MS-DOS	Red hat Linux	Mac OS
Mac OS X	Sun Solaris	System V UNIX
HP-UX	Other proprietary UNIX	Other open-source UNIX
OpenBSD	Other BSD UNIX	Mandrake Linux
SuSE Linux	Other Linux	OS/2

Amiga

24 percent responded with 95/98/ME computers being used as their desktop system (Misterpoll, 12/4/2001). An independent web site for information on rare coins dans www site, collects and publishes information about access to this web site. The sites server statistics indicates a "Distinct hosts serverd:" rate of 2641 host per day (Dan's www site, 8/28/2002). The distribution of operating systems shows that 58 percent of accesses are by Window 95/98/ME operating systems (Dan's WWW Site, 8/23/2002). Because of the nature of the website I will make the assumption that the majority of the accesses are coming from home computer users. On 31 March 2002 Global Reach, a firm that provides demographic information related to consumerism and the web indicated that there were 560 million people on line (Global Reach, 3/31/2002). Assuming that half the people are business users and the other half are home users you have (.24 x 280m + .58 x 280m)= 229 million windows 95/98/ME computers on the internet potentially waiting to be attacked and have information stolen or used as attack platforms against other computers.

What does a secure computer looks like

What does a secure computer or network system look like? Using the principal of "Defense in Depth" (Sans, 2001) it is one in which multiple layers of defenses are put into place, around information or an environment that you want to protect.

The first layer of protection is understanding the risks involved with having a computer or networked system connected to the internet. Risk can be defined as a function of threats, (worms, virus, denial of service, malicious users) and vulnerabilities, (flaws in software, implemented network process, freely observable data transmissions, users acting in a manner that's contradictive to safe computing). A formulaic view is that RISK = THREAT X VULNERABILITY (Sans, 2001). Vulnerabilities to a computer system can be measured by running available vulnerability scanners that look for those vulnerabilities to known threats, such as open ports, file shares, and unpatched network software. After understanding the risks associated with being connect to the Internet. A decision is made to accept, mitigate or transfer the risk. With the mitigation choice leading to the next layer of a secure system.

The second layer of protection is to apply available patches and security updates to a computers software suit before it is connected to the Internet or as patches become available. Patches usually fall in the area of the network protocol drivers. Many protocol drivers were designed before the threat to network connected computers was as prevalent as it is today. An example of an unpatched protocol driver is the driver that is responsible for the transport layer of the TCP/IP stack. In this layer data that is inside the packet is received and accumulated for delivery to the system. If you receive more data than the buffer was designed to handle you get what is called a buffer overflow. A buffer

overflow is where data gets written into memory locations that should not be written to. The problem with this is that you do not know what will happen if this data gets executed. In the early days of networking, no one expected a computer to send anything but normal packets so no tests were done to prevent buffer overflows from happening. Today though, many of these types of problems have been discovered and corrections to software have been made to prevent this type of problem for occurring. Also today there are groups of people looking for and reporting new problems that are being discovered. With each new problem there are new patches being created to solve these problems.

The third layer of protection is attempting to prevent hostile attack from reaching a computer or network system. The first method is preventing, detecting and eradicating viruses, worms, and Trojan horses and any other malicious software. Antivirus software is the front line defense against these types of attacks. Currently there are proximally 62000 known virus and worms that antivirus software detects. By keeping updated antivirus software on a computer, many stand-alone programs used by hackers to corrupt or take control of a system can be prevented. A second vector of attack is through the Internet connection itself. By placing a firewall between the system to be protected and the external Internet with rules set to deny all access except those that are necessary for minimum operation you will reduce the number of threats to that system. A third vector of attack is from direct console access by users. A user operating with malicious intent can delete or modify data. They can introduce software on to a system that decodes passwords, records keystrokes, creates back door connections, or en wholesale destroys what ever is on the computer. Having systems that have password-protected access and requiring users to login further reduces the number of user access vulnerabilities. Additional requirements for this level of protection to work are regular reviews of firewall settings; logs of network traffic and requiring users to use strong passwords that are being changed regularly. These requirements are actually covered in other areas of protection.

The next several layers are hard to place in numeric order because they tend to be simultaneous in the way that they are used. For continuity of flow of I will take license and number them.

The fourth layer of protection is intrusion detection. Intrusion detection can at times look like an art form. On computers with good logging capability a tremendous about of information is available about what the computer is doing and how it is being used. This information can be gathered directly at the host for host base intrusion detection, or from firewall logs and direct network monitoring for network intrusion detection. The problem with intrusion detection is that there is a lot of data that has to be looked through, and this is where the art form comes in to play. To detect intrusions on a given host that are not blocked by the firewall operations or the antivirus software, you have monitor log files and network connections for unusual activity. By monitoring login logs and

observing who and when a user logs in you can spot unusual activities such as a user logging in after normal hours. By monitoring file access logs you can find those cases were a user is accessing a file and modifying it when there is no reason for this activity, such as deleting and copying files, making changes to an operating system executable or dll. To automate much of the log monitoring process, there are sensor programs that can be tailored to look at logs for these events. Also at the host level of intrusion detection you monitor network traffic coming into the system. With host base or network base Intrusion detection software, packet information is compare against a know set of signatures making much of intrusion detection automatic. By logging as much information as is reasonable for the computer you can generate enough information to detect a large number of intrusions that go undetected otherwise. With network intrusion detection you are monitoring all network traffic as it propagates through your network. You can monitor traffic before and after the firewall. By monitoring in both locations this helps determine how well your firewall is working for you. Even though there is detection software monitor the network you still have to monitor the firewall logs for what traffic was or was not permitted looking for unusual traffic. The kinds of traffic you are looking for is, network packets that originate outside your network that should only be coming for within. You are looking for TCP/IP control flags that are used in combination that should not be used together. You are looking for packets that cause buffer overflows, or cause the network interface to behave differently then intended. You are looking for any packet that does not fit the normal format of a TCP/IP data packet.

The fifth layer of protection is auditing. Auditing is the process of taking a snap shot of a system as it is so that it can be compared to what it was. In order to know when something is different you must know what it looks like before it changes. An initial baseline of the system must be taken first to provide a reference to compare with later audits. Information that is collected should include the list of authorized users, current registry setting, network ports that are in use, running services, information about the file system, information about data files, all logs that are available. In other words as much information about the current state of the computer as possible. After the initial base line has been collected regular audits must be conducted, with each audit being compared against the baseline looking for changes. By coordinating change information generated by the comparisons can determine weather a change was authorized or not authorized. In this manner you can verify the integrity of the system and verify that no unauthorized access or changes have taken place.

The sixth layer of protection is policy. Policy is the written rules defining as many aspects of computer operation as are necessary for the situation that the system is being used in. You can have one policy statement covering all aspects of the computers operations or you can have several policies tailored for various conditions and user responsibilities. The policy or policies determine who has access to a system, what privileges they have, what software is allowed to be installed, who is allowed to install it, how often is antivirus software run on the

system, how often is it updated, what network connects are allowed by the firewall, what log information is to be collected, how often is it looked at, how and when are audits conducted, and what is to be done when discrepancies are detected. As you can see there are considerable areas that have to be though out and determinations made how to handle each. With a well written policy or set of policies the What, Where, When, Why, how and who, can answered for all questions that make managing a secure computer system possible.

Now that I have defined what is needed to make a computer system secure lets looks look at what is necessary to make a windows 95/98/ME computer system secure. Because there is a considerable overlap, in terms of security, between a win9x computer used for home versus small business use, I will start each section topic discussing the common features first then add in specific features that need to be added to fit the home or business environment.

What available tools are there are?
When looking at securing a win9x environment you need to understand the threats that are being applied to vulnerabilities that exist with this system. For home and business users there are common threats of viral, worm, Trojan, and denial of service attacks. For the business users there are additional threats that come for internal sources such as malicious and dishonest users. To get an Idea of the types of threats that are present and what systems they affect you can go to http://www.cert.org/. When the decision is reached to mitigate such threats. CERT at Carnegie Mellon recommends that you install patches available from Microsoft, install antivirsus software, and install a firewall of some type (Cert, 4/17/2000).

The second layer of protection for win95 computers is located at http://www.microsoft.com/windows95/downloads/ this is the list of updates and patches that are available. All users business and home should as a minimum install; Windows Service Pack1, Dial Up Networking 1.3 Performance & Security Update, Dial Up Networking 1.3 and Winsock2 Year 2000 Update, Windows Socket Update – Kernel 32, Windows Socket 2 Update, Winsock/DNS Upgrade 1.2 for pptp, Windows 95 Year 2000 Update, Windows Share Level Password Update, and all Critical Updates and all Security Updates.

To get the second layer of protection for win98/win98se/winme computers you will have to be online to use the Microsoft automated windows update utility at http://v4.windowsupdate.microsoft.com/en/default.asp when you click on the 'SCAN FOR UPDATES' button, it will determine what version of windows you have and find available updates for your computer then apply them. The problem that I see with this is that you have to connect an un-updated computer to the Internet first, exposing it to attack while you are waiting for updates and patch to be applied. Also depending on your connection speed, dialup users could be waiting a considerable time. After the operating system updates and patches have been applied, install the most current version of Internet explorer. This can

be found at http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/default.asp then hit the 'GO' button.
Also for win98/ME computers that are going to be remotely accessing a network capable of IPSEC secure connections, support for L2TP/IPSEC should be installed, this is located at http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp This provides support for layer 2 tunneling protocol and IPSEC for VPN over the internet.

After the patches and security updates have been applied you can then address the second layer of protect of, how to prevent hostile attack for reaching the computer or network system? Antivirus software should be installed on any computer even if it is not connect to the internet. There are many commercial vendors of antivirus software including Symantec with Norton antivirus, Network Associates with McAfee. There are also freeware sources of antivirus such as AVG antivirus located at http://www.grisoft.com/html/us_index.htm?session=433167b99b8c7f248547d77eabfe23f2 . Along with antivirus software, personal firewall software for the single computer should be installed. Sygate produces a very good firewall with intrusion detection capabilities. The use of this firewall will also satisfy some of your requirements for producing logs that will be used later on at higher layers of defense. Sygate is located at http://soho.sygate.com/products/pspf_ov.htm. For small business that may have several computers connect to a network it would be good practice to include a single computer to act as a gateway to the Internet. On this machine better firewall software can be installed and example would be BlackIce defender. Blackice is a combination firewall and intrusion detection software. One of the outstanding features of this software is that it uses statefull inspection of packets. Stateful inspection means each packet is inspected to determine what it is doing before applying the firewall rules. This will help prevent an attacker or user from trying to use a communication method that is nonstandard i.e. attempting to run or access a web site on ports other than 80. Blackice is located at http://blackice.iss.net/product_pc_protection.php. Now that the firewall is protecting the computer from outside network attacks lets see what can be done to prevent user attacks. One method is to require all users to log on to a system. With win95/98/Me computers you can bypass the login screen simple by hitting the cancel button that's located at the login prompt. To prevent this from happing you can install software such as Winblocked by RSS Systems. Winblocked is a single user locking software that prevents a user from bypassing the logon screen. Also winblocked uses encrypted password storage to make it very difficult for your password to be stolen and used. It is located at http://www.4diskclean.com/winblocked.htm. Another software package that will password protect logon and has lockable screen saver and provides multi-user support is SafeLogon by Gemiscorp. This program when installed will require a user to supply a password when logging on. It disables methods of bypassing user logon, provides secure screen saver operation, logs user logon, and is compatible with windows password system. One advantage of is that fact that it

will produce logon/logoff logs. Safe logon is located at http://www.gemiscorp.com/english/main.html. . Another method of protection against unauthorized users is files encryption. File encryption can also be used as a method of protection, in a small business when not all employees need to be able to read all information. Strong disk Information Security Systems has a program called Strong Disk. Strong disk works by creating a virtual disk drive that is encrypted with triple DES, CAST 128, SAFER, or Blowfish. All data in the logical disk is encrypted and decrypted using two keys. The first key is a long binary combination randomly created and the second key is a password of your choice. The long key is stored as a trinket file that can be placed on a floppy, cd, or other small data storage device designed to store a key code, and removed from the system. Strong disk can create multiple virtual drives each with it own password. Strong disk is located at http://www.strongdisk.com/. To allow multiuse control of file access without encryption there is Access Administrator Pro. This program modifies the system kernel to provide NTFS like file access control. Access Administrator Pro is located at http://www.softheap.com/acadmpro.html.

At this point the single computer or networked computers vulnerabilities have been reduced, providing reasonable protection from a large number of threats. With all that has been done there is still the possibility of unauthorized access to the computer or system. In the fourth layer of defense you look at intrusion detection. Intrusion detection is the process of observing a computer or network systems operation and by understanding what is normal and what is not determining weather an intrusion has occurred. Software for this purpose is available that will automatically monitor network traffic, for known signatures of abnormal traffic and look at log files for abnormalities then give an alert that something is wrong. With win95/98/Me much of the information that is needed to successfully monitory a computer system for intrusions is missing. At this point the solution to this problem has been solved by many of the steps that have already been taken. With SafeLogon you now have logon and logoff logging. With Sygate firewall you have added direct host base intrusion detection with network monitoring and logging of network traffic. With Access Administrator Pro you have logging of files access and registry access. To get information about what registry keys were actually changed you can use regmon. Regmon monitors the registry and indicates what processes are accessing the registry and what changes they are making. Regmon also has filter capability allowing you to configure it to monitor processes of your choosing and it provides logging capability. Regmon is located at. http://www.sysinternals.com/ntw2k/source/regmon.shtml. Now that you have logging and are collecting a tremendous amount of data you need to look at it for the unusual. Currently I have not found any programs like Dragon Squire or RealSecure. These two products are sensors. They look at log files looking for signatures of events to indicate an intrusion. To accomplish this on win95/98/ME you will have to manually look at the logs produced by the security products installed and look for odd events yourself. In the Login log you will be looking for excess login failures, users logging in at odd hours, users logging in as accounts

that should not be logging in because the user is away. In the file access logs you need to know what users should be using what files. If you have installed Access Administrator Pro each user can have areas that accessible and others that are not. It is the areas that a user should not have access to that triggers the alarm in your mind that something is wrong. When looking at the registry logs you are looking for unknown applications that are making changes to keys and values. You are looking for additions to the "run", "run once" and "run service" that are not expected. You also need to look for the registry editor being used to make changes during times when it should not be running.

The fifth layer of protecting a windows 95/98/Me computer is Auditing. The National State Auditors Association and the U.S. General Accounting Office consider Auditing for Information systems Security so important that they have created a 66-page document outlining the process for auditing an information system in terms of its security (National state Auditors Association and the U.S. general Account Office, 12/10/2001). For the home or small business user the audit is a very useful method to determine if changes have occurred that are unexpected. Where the unexpected change could be due to an intruder having accessed the system in a manner that was not detected by all the previous steps taken to prevent unauthorized access. Areas that should be audited should include, the list of authorized users, the list of open TCP/IP ports, the list of running services, current registry settings, and the current state of all important data and operating system files. To begin auditing a system you must first take a baseline audit. This will be the state of the system that will be compared to the next audit. The list of users is not easily collected but can be found by looking for files marked pwl. These are the password files that were used by a user when logging on. Next using netstat/all you can get a list of all TCP/IP ports that are in use. Save this list to a text file. Next you need a list of all running programs and dlls. Using listdlls by sysinternals the lists of load dlls can be gotten, save this file into a text file. Listdlls is located at http://www.sysinternals.com/ntw2k/freeware/listdlls.shtml. To get a text output of the registry use regedit and select the HKEY_LOCAL_MACHINE then under file hit export file this will produce a text copy of the registry. Also you need to select HKEY_USERS and perform the same export. To get information about files you can use a program called File Guardian - 1.0. The primary purpose of this program is to record the state of specified files and automatically restore them to their original condition if changes occur, it can be adjusted to produce a log of the current state of files. With the base line audit completed the next audit will be compared against the baseline for unauthorized changes. One tool that can be used to check for changes within the audit logs is Filecomp. Filecomp is text comparison program that can be used to show differences between two text files. After the comparisons of all the audit files have been made you still have to look at the differences to decide weather they are due to normal process or due to an unauthorized intrusion into your system.

The sixth layer of protecting a windows 95/98/Me computer is writing a policy or a set of policies to govern how the computer is to be used. A policy can be a very useful tool in protecting a computer system. One author states "Security policies are important to protect information and systems from misuse by people within the organization and to prevent users from unwittingly providing access to outsiders" (Tim McCollum, 8/15/2002). For a home computer user, one police statement should be concerning using passwords to access the computer and choosing passwords that are considered strong. A strong password is one that is usually at least 8 charters long and has a mixture of upper and lower case letters, numbers and special characters. Also the password should not use common words that occur in a dictionary. To make a password strong with consideration for the Microsoft LAN Manager password storage scheme, the password should be considered to be made up of two 7 character long passwords joined together. Each 7 character segment should follow the rules for strong passwords. A second police statement should be that the computer will have antiviruse software installed on it. The antivirus software will be updated at regular intervals, say weekly. Antivirus scans will be performed regularly weekly also and that no software will be loaded without scanning for virus. What to do in the event of virus infection. A third policy statement should say no peer to peer file sharing software will be installed. Although it practicality people are going to use these programs which means more effort on the part of the user to be sure that they have not open the system up to compromise. Before continuing with policy statements, assuming that a home user is going to install peer to peer software. An audit of installed software should be done before installation. Then after installation a second audit should done. Than look to see what was installed. I have seen that many of these programs, install adware programs that come from companies who are funding the peer to peer authors. Some of these bundled programs look like "Gator, Adcompanion, Offercompanion, Bonzi Buddy, and several others". These programs monitor a users web browsing looking for keywords to convert to active links to a sponsoring company's web site. They also collect information about what websites are visited and forward that information too. A fourth statement should be regular audits will be conducted on a monthly basis. A fifth statement should be what to do in the event of intrusion detection. For this policy statement you can get information on how to report a computer crime at http://www.cybercrime.gov/reporting.htm. Also in order to more effectively prosecute a criminal, a warning banner should be used

"**WARNING**WARNING**WARNING**WARNING**WARNING**WARNING

This {Your State Here} computer system is provided for Official Use Only. Any information placed in the system belongs to {Your State or Agency Here} and may be monitored, used or and disclosed by authorized personnel. The data on the system may be searched at the request of law enforcement or other persons, as appropriate, and may be disclosed and used for disciplinary or civil action or criminal prosecution. Use of this computer system constitutes consent to these policies.

THERE IS NO RIGHT TO PRIVACY IN THIS SYSTEM.

WARNINGWARNING**WARNING**WARNING**WARNING**WARNING"

(DOJ)

This banner was taken from state government guidelines for computer use and should be adjusted for home or small business use. For the average home user this should allow them a reasonable amount of Internet freedom with a reasonable amount of risk. For the small business user they need to use all the statements above and add additional statements. This includes, Do not give out you password to other users, Do not load software without permission, Do not load peer to peer software, Antivirus scans will be conducted daily, Who is responsible for viral prevention and eradication, The firewall will be set for minimum service except those that are needed for operation, Who is responsible for system administration, What is to be done in the event of an intrusion in terms of making backup copies of suspect systems, collecting all available logs for analysis as to how the intrusion occurred and by who, and then taking steps to restore the system back to functional with patches to prevent further compromise. For the small business this should allow them a reasonable amount of protection from external and internal attacks and prepare them to prosecute those individuals who have committed a crime.

My final topic User Responsibility
What are the user responsibilities necessary for maintaining a secure computer system? All users weather home or small business are responsible for physical security of the computer. For the home user some physical security comes from the homes security, by locking the house when away from home and monitoring who is using the computer many unauthorized uses can be prevented. For the business user computers should be behind lockable doors to prevent a person from walking up to the computer and attempting some physical method of accessing data or other network information. For both home and business each user must create and use strong passwords. The password should be changed regularly, such as every 60 to 90 days. Users should not install potentially dangerous software such as file sharing programs like Kazaa, Winmx, gnutella, and morpheus just to mention a few. These programs in them selves are not dangerous but in there operation they contact other computers that you have no control over. They also can be a source for violating firewall policy by responding to requests for connections to unknown computers via a central control host computer that your client computer is communicating with. All users should make sure the antivirus software is update and they should virus scan all software downloaded from the Internet before installing on their computer. Users also need to pay attention to there computers operation. How often do you hear reports of a user saying, the computer did something funny, or its running slower than usually, or something else out of the ordinary happened and then finding out

that the behavior was due to a virus of some type. The most important thing that a user can do is following the policy that was setup to protect the computer.

Conclusions

Windows 95/98/Me computers have very little security built in to them. By installing a variety of 3rd party software programs, many of aspects of a secure system can be implemented, allowing a windows 95/98/ME computer to operate in a hostile environment with significantly reduced risk of compromise.

References

Cert, "Windows 95/98 Computer Security Information." 4/17/2000. http://www.cert.org/tech_tips/win-95-info.html - f.1. (8/20/2002

Dan's WWW Site, "Distribution of OS's." 8/23/2002. http://65.187.212.145/os.asp (8/23/2002).

Dan's www site, "General Summary, Distinct hosts served." 8/28/2002. http://65.187.212.145/analog/Report.html#Rep3 (8/28/2002)

DOJ, Approved Logon Warning Banners http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.htm (8/25/2002)

Global Reach, "Global Internet Statistics (by language)." 3/31/2002. http://www.glreach.com/globstats/ (9/10/2002)

Misterpoll, "Workplace Operating Systems." 12/4/2001. http://www.misterpoll.com/results.mpl?id=1657704867 (8/28/2002)

National state Auditors Association and the U.S. general Account Office, "Information Systems Security auditing." 12/10/2001. http://www.gao.gov/special.pubs/mgmtpln.pdf (9/12/2002)

Sans, "defense in depth", 2001. SE_21

Sans, Phil Bandy, Michael Money & Karen Worstell, "Intrusion Detection FAQ." 2000. http://www.sans.org/newlook/resources/IDFAQ/ID_required.htm (8/22/2002)

Tim McCollum, "Managing Security Policies." 8/15/2002. http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=477 (8/20/2002)

U.S Department of Justice, 7/2002. http://www.usdoj.gov/jmd/irm/imss/2002itplan/strategic_plan.htm - 5 (9/12/2002)

usdoj-crm/mis/krr, "Computer Crime and Intellectual Property Section." 9/6/2002. http://www.cybercrime.gov/reporting.htm (10/10/2002)