Global Information Assurance Certification Paper

Thomas L. Gillikin

Advanced Incident Handling Practical

"The internal threat to Virtual Private Networks"

Summary

On December 8th a Computer Incident Response Team member noticed an unusual log entry on a network intrusion detection system (IDS) which was monitoring a virtual private network (VPN). The log seemed to indicate an intrusion in the network. Upon closer review he determined someone had conducted a classic brute force intrusion into a portion of the VPN. The Solaris and Windows NT victim network had current patches and service packs and was monitored by three Intrusion Detection Systems (IDS) at three separate locations. The first (IDS1) was at the victim site. The second (IDS2) was at a VPN communications center and the third (IDS3) was at the CIRT. One of the activities the IDS were programmed to record were sessions that had unsuccessful logins. In this incident, the intruder guessed twenty default passwords on at least 5 different systems and succeeded on his twenty first attempt. The intruder correctly guessed a root password that was literally "abc123". Personnel reviewing the IDS logs at the first and second sites did not detect the intrusion. A check of the offending IP addresses indicated they were registered to segment of the VPN at another site a considerable distance (several thousand miles) from the victim system. Initially, several possible theories for this scenario were considered including the suspect IP addresses was being spoofed and another area of the VPN had been compromised and was being used to launch the attack that was detected. None of the initially discussed scenarios proved to be correct. However, all IDS and network analysis seemed to show the attack originated from a site located physically near the victim VPN and routed through the same communications center used by both sites. This gave us the unusual situation where we had IDS logs showing, with a high degree of confidence, where the attack originated. However, this conflicted with IP registration information. When we contacted the Florida site where the suspect IP was registered, we were told the IP was assigned to another site in the area of the victim. The communications center was using other IDS systems that were monitoring traffic from outside the region. No other unauthorized activity was seen by IDS1, 2, 3 or any other IDS. This caused us to believe that the attack originated at a specific, known

point within our VPN and not from outside. The consensus was if the attack was from the outside (the VPN), then one of the other IDS would have probably detected it. Therefore, we were able to determine the intrusion came from a portion of the VPN in the same geographical region as the victim site.

I was a member of a team of two law enforcement officers, trained in network intrusions that were sent to the victim site to conduct an investigation and assist the CIRT in determining appropriate technical response.

Preparation Phase

The victim site was located in a remote area of the world and required nearly two days (42 consecutive hours) of travel for the response team to arrive. The team had experience and training in computer forensic processing, monitoring, intrusion detection, and incident analysis. We also were well training regarding the established procedures to systematically identify, collect, protect and analyze computer related evidence of violations of law. The team utilized the unusually long travel time to specifically plan and tailor the investigation to the specifics of this incident. Previously created generic checklists were modified to address issues regarding this particular case. We identified our specifically assigned tasks, then planned and coordinated our efforts.

As team leader, I served as the primary point of contact for the response team to the senior management. Communication between the CIRT and the response team was conducted via telephone or PGP encrypted email over another network, thus diminishing the chances of anyone reading our e-mail.

We carried all the equipment required to conduct an appropriate investigation. We knew that the required equipment or spare parts would not be available locally. The emergency response kit was tailored to the Solaris and Windows NT operating systems. Particularly useful was a Compact Disk (CD) containing binary files known to be unaltered. This would be useful if binary files were suspected of being modified by the hacker to ignore his activity.

All systems have a banner which informs users that the use of the system constitutes voluntary consent to monitoring and that any or all activity shall be provided to Law

Enforcement (LE) if management deems it necessary or if requested by LE.

Banners usually are worded in a format similar to the following:

> THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAIN UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THE SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USE FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

All monitoring was done in strict compliance with the Electronic Communications Privacy Act (ECPA) and was coordinated closely with appropriate legal authorities. These procedures are established by internal policy as well as law (U. S. Federal Code Title 18). Basically, the ECPA says system administrators are allowed to monitor their own systems and networks if the monitoring is necessary to properly administer, maintain and/or protect the integrity or reliability of their system.

TITLE 18 CRIMES AND CRIMINAL PROCEDURES in CHAPTER 119. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS.

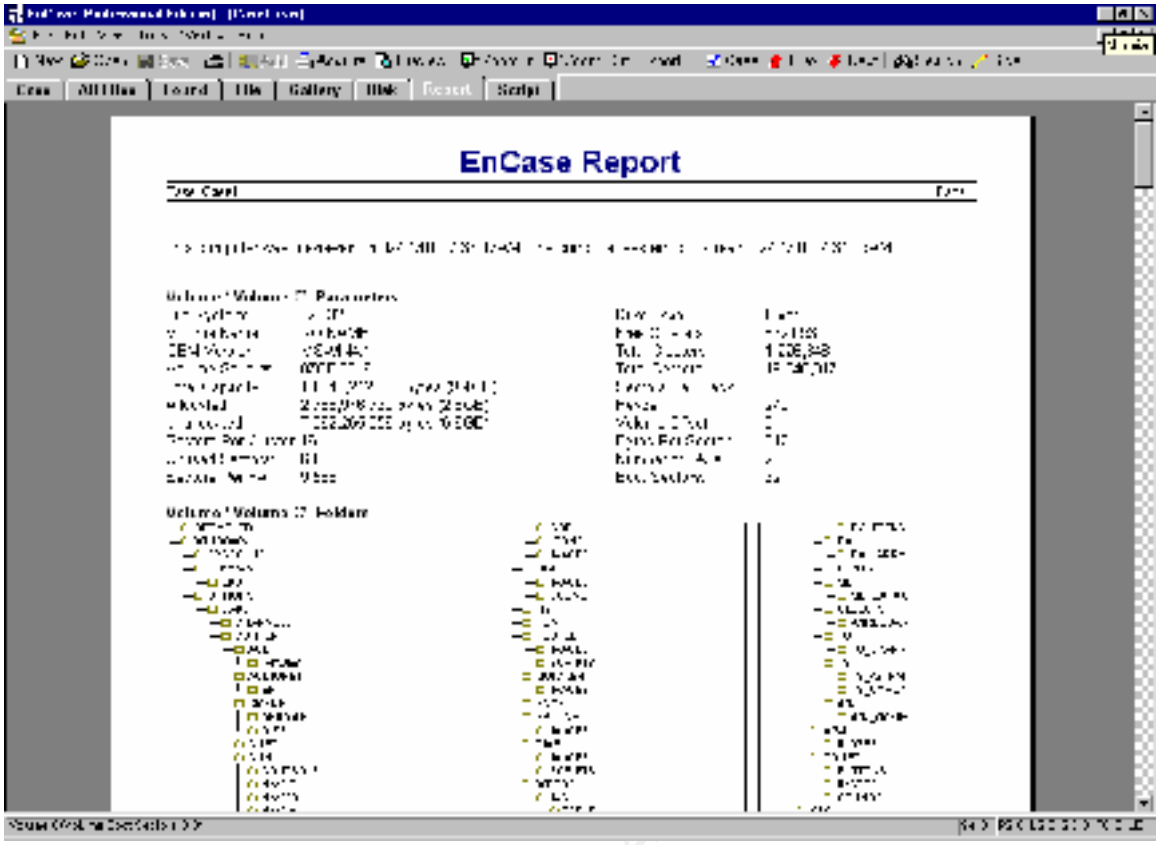
2) (a) (i) It shall not be unlawful under this chapter [18 USC §§ 2510 et seq.] for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic

communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

The Electronic Communications Privacy Act (ECPA) of 1986 was adopted to address privacy issues that were evolving with the growing use of electronic communications. The ECPA is designed to clarify what constitutes invasion of privacy when electronic surveillance is involved. It extended privacy protection outlined in the earlier laws and to comply with current case law regarding computers and electronic communications. ECPA has been amended several times since it initially became law in an attempt to keep pace with changing technology. The ECPA prohibits an employer from monitoring employee telephone calls or electronic mail when employees have a reasonable expectation of privacy. Generally, the Act does allow employers to monitor and record these activities if employees are using the employer's network or equipment and the employee is notified in advance of the monitoring. This is normally done by using "banners" or by user agreements or a combination of both. Both are a written notice of the employer's intent to monitor the employee's activities on the network. The banner is displayed every time a user logs into a computer system. Employees are usually required to sign the user agreement before they are allowed to access the computer system.

Generally, if the a banner is not be installed on a particular port, then monitoring may not be conducted without further legal steps. Usually a banner may be accomplished on each system by using "TCP Wrappers". However, court decisions may alter an employer's legal authority to monitor. Therefore, it is a good idea to always check with your legal advisor prior to the start of any monitoring.

For remote communications, each team member was equipped with a cell phone/pager capable of receiving voice mail and e-mail. Contingency plans must be in place if the team is required to travel internationally, as most cell telephones are not compatible to every cellular system world wide. Preparation must start months in advance of an incident and



continue until the response begins. It is a continuous process that must be reevaluated and modified regularly.

My favorite forensic tools are from two sources. The first is "Maresware" (www.dmares.com) which is a collection of over 56, 16 bit tools and 21, 32 bit tools. The second is "Encase" (www.guidancesoftware.com) a GUI based forensic tool that dramatically reduces the time needed to rapidly glean useful information from disks. These tools are maintained either on CD, laptop computers or floppy disks. The following is an example of one of the Encase screens:

Jump bags should also contain a copy of "Safeback." Safeback is used to conduct a backup of all data on a physical hard drive. Fresh backup media should also be in your bag. I have been to several incidents where the only backup media the victim site had were the tapes that they used to backup their system. These tapes were generally worn out and are not be adequate for forensic use. Also, a small hub and a laptop computer with dual operating systems should be included. I have also found it useful to carry 4 – 6 IDE hard drives. Experience has taught me that courts prefer original evidence. A copy of a hard drive, even if it is identical to the original, is less desirable and gives the defense

ammunition during the trial. System administrators are reluctant to give up a hard drive unless there is an immediate replacement available. Another good thing to carry is a call list with the telephone numbers of everyone in your organization, including home telephone numbers. Appendix 1 has a brief description of some of the other tools I routinely carry when I respond to an incident. It was not necessary to use any of the listed tools in this incident.

Identification

Initial detection was made by a member of the Computer Incident Response Team who was assigned to read and evaluate intrusion detection system log files. This is the point that the incident handler started his notes, describing exactly what happened, when it happened and what action was taken. Notes are critical to appropriate incident response and building a successful prosecution. Although the victim network was monitored by three Network intrusion Detection systems he was the only person to recognize the attack and subsequent intrusion. All three IDS systems were designed and configured to monitor the network for known vulnerabilities and attacks. The initial weak link ultimately became the analysts who must be trusted to read the log files and interpret the captured logs. The sheer size of many IDS log files may discourage or overwhelm many incident handlers. In this incident the reviewer maintained his situational awareness and made sure he had up to date information regarding the environment where the victim network was maintained. He knew the system was suffering from poor performance. So he paid particular attention to the session when the failed login was recorded.

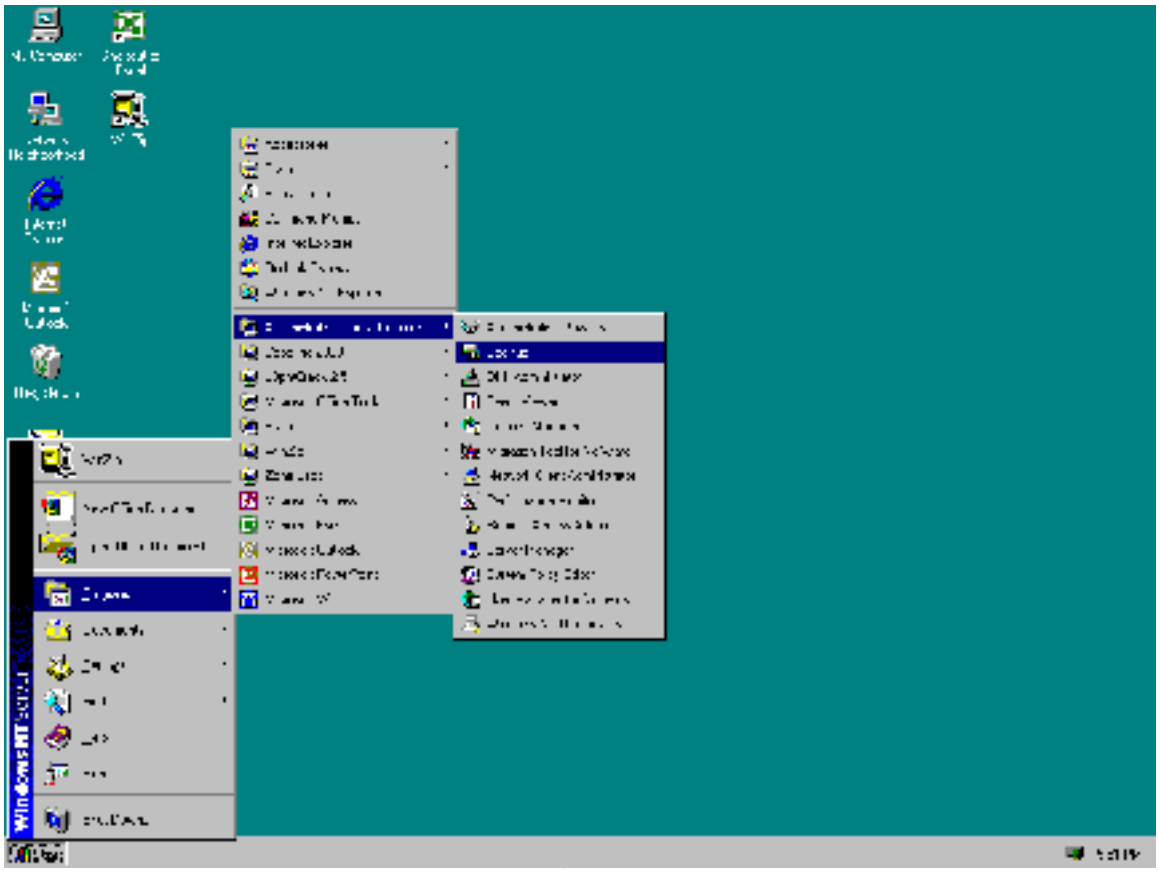
When he identified the intrusion, he immediately was designated as the primary incident handler and notified his supervisor (who was also the head of the Incident Response Team). The leadership of security and line management were kept in the information loop. This minimized the chance of inappropriate or ineffective response. In this particular case, the log reviewer noticed a session was recorded when what seemed to be an authorized user, entered an incorrect password to gain root access to the victim network. While an incorrect password entry is not unusual, a telnet, coupled with the 20 failed attempts at logging on directly as root attracted the reviewers attention. Logging on as root via a telnet session is rarely, if ever, a good idea

because such transactions are easily intercepted (sniffed) and logging in as root is supposed to be prohibited by default. The result of direct logging to root is the root password may be captured by a hacker and he can then easily take over your network. In this case, the intruder seemed to be guessing default passwords on a number of systems. On the twenty first try, he succeeded in gaining root access to a system on the network. He then proceeded to check trust relationships and using these relationships, made his way to the primary domain controller (PDC). The intruder looked at several processes and files (but not the SAM file) then exited the system. He stayed in the PDC for exactly 90 seconds and exited his way back out the system the way he had come. He did no damage, nor did he alter any files, upload/download software or add any accounts. He made no attempt to hide his unauthorized entry and was not detected trying to return to the network..

Containment

Because of the remote location of the victim system, containment was undertaken remotely. The local VPN provider was notified of the incident and (by prior agreement) immediately severed connectivity with the rest of the VPN. This was done primarily for two reasons. First, to deny to the hacker the opportunity to re-enter the victim network. Secondly, to prohibit access of the remainder of the VPN if he decided to continue his attacks. System backup was conducted by the system administrators prior to the arrival of the Response Team. Tape backup is a relatively simple process in the Windows NT environment. However, experience has taught me to always request the backup be completed on new, unused tapes with the verify block checked. I have learned the hard way that unless these two simple steps are followed, I would sometimes receive a blank or unreadable backup tape. It is advisable that the backup tapes be used to restore the victim system onto different hard drives. A taped backup is not a substitute for an appropriate, thorough forensic examination of a hard drive. In most situations, I recommend backing up the hacked system, pulling the hacked hard drive and placing it into evidence. Then the administrator should restore the system from backup tapes. Needless to say, the backup used to restore the system should be the last backup before the intrusion. Otherwise, the hacker will just use the same vulnerability to regain access.

The system administrator of the victim network was notified by telephone of his problem. He was aware of his network difficulties (slow performance and runaway processes), but was not aware of the network intrusion. The system administrator was informed that a team was being sent to investigate the intrusion. He was asked to tell only those with a need to know about the pending arrival of the two law enforcement officers. Unfortunately, the word spread like wildfire and the element of surprise was completely lost. He was also directed to secure the network area and prohibit, or at least minimize physical access to the network. The network was removed from the VPN, binaries from a trusted source (CD) were loaded and used to run a complete backup with verify, for each computer in the network. The backup tapes were stored securely until they were turned over to the response team leader. Only one tape was made for each system and the original hard drives were not saved. They were reused for the reinstallation of the system prior to the arrival of the CIRT members. All passwords were changed and assigned by the network security officer. A screen shot of the steps to take in a Windows NT system are included below:



The system administrator was provided a copy of the intrusion response check list based on the Carnegie Mellon University model and the eradication process was begun. Additional incident response help was provided by information retrieved from www.cert.org as well as SANS at www.sans.org. Both sites contain a wealth of information.

If the victim system is Solaris, I recommend using the following command to data dump all information on a fresh tape:

```
#dd if=/dev/rdsk/c0t0d0s2 of=/dev/rmt/0
```

This command will make a bit copy of the entire system and place a copy of the file system to the SCSI rewindable magnetic tape known as /dev/rmt/0. This data dump may take a number of hours (depending on the size of the physical hard drive.

Another command that should be used (for Solaris systems) is:

#tar –cvp /dev/rmt/0 ./proc

This command will archive processes running in memory. Make sure you run this command before shutting down the victim system. Otherwise, you will loose valuable data. I have seen incidents where hackers have downloaded their tools, started them then deleted their tool files from the system. If the system is rebooted, there will be no trace of their activity.

Throughout this process the Network Intrusion Detection systems continued to monitor the effected networks. No other unauthorized activity was seen.

Eradication

This intrusion was exceptionally straight forward. The system administrator who originally installed the NT operating systems failed to change all of the default passwords. A network is only as strong as it's weakest system. This oversight resulted in a significant amount of painstaking work to confirm that the hacker had not modified any files on the victim systems. Although the hacker was caught by the IDS, we were not absolutely sure that this was his first visit to our system. Nor were we sure that another hacker had not found his way into the network using the same attack method. Therefore, all passwords were changed and all administrator and user accounts verified. Additionally, system names and IP addresses were changed and a vulnerability analysis was conducted remotely by the CIRT. Just to be on the safe side, all networks at the victim site were examined. A number of improvement areas were noted and corrections were made.

System log file on the attacking system were located and analyzed and the number of potential hackers were narrowed to one person. He was the only person logged into the suspect system during the time of the hack. The hacker was a system administrator at the suspect site. He had an excellent reputation for his technical ability. As I said earlier, word of the arrival of the two law enforcement officers spread like wildfire. He heard the law enforcement team was at the victim site and was planning to come to his office. He went to his supervisor and admitted hacking into the other network. When we arrived, he was prepared to assist us in identifying

exactly what he did and how he did it. He said he had heard that the victim system was having a problem with performance caused by runaway processes. He said he thought he could correct the problem. When he hacked into the PDC he realized the problem was not what he thought it was, and exited the system. He said no one had ever told him he was prohibited from entering a network not assigned to him. The case was presented to the Attorneys and it was decided he would not be criminally prosecuted. He was administratively disciplined.

Recovery

Our organization's policy is to conduct a vulnerability assessment following any intrusion. System administrators are usually eager to have their system evaluated and secured after the significant amount of time they spend recovering from an intrusion. It is a experience they never want to got thorough again and anything that can minimize their risk and exposure is generally welcome. The hacker showed us step, by step, how he exploited the default passwords and trusted relationships to work his way through the network. In addition to changing all the passwords, each trusted relationship was evaluated to determine if it was really necessary. Most of them were not and they were eliminated. The recovery phase was completed on December 22 and the network was placed back in service. The victim network was out of service for 14 days.

Follow up/Lessons Learned

At the conclusion of the field work, a detailed written report was compiled regarding the incident. All notes from the beginning were included as an attachment to the report. Unfortunately, the IDS logs were inadvertently destroyed.

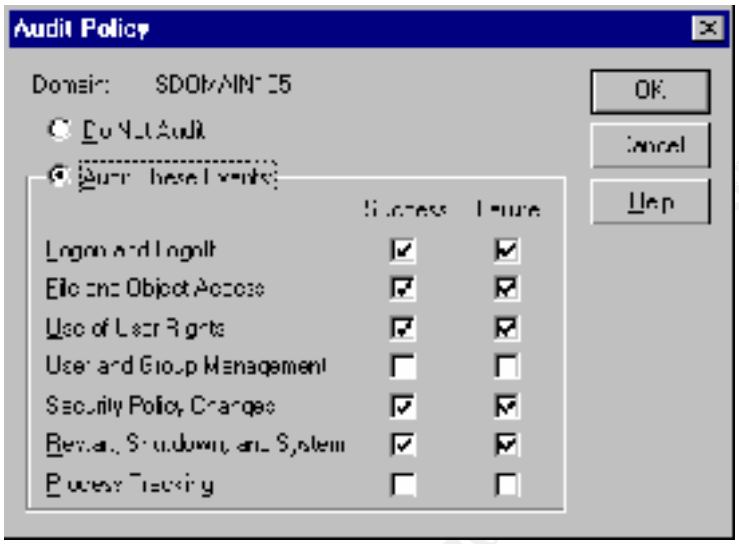
The following are some of the lessons learned in this incident:

A. Additional training was required for system administrators to make sure they understand they must not enter portions of the VPN for which they are not responsible and do not have an authorized user account.

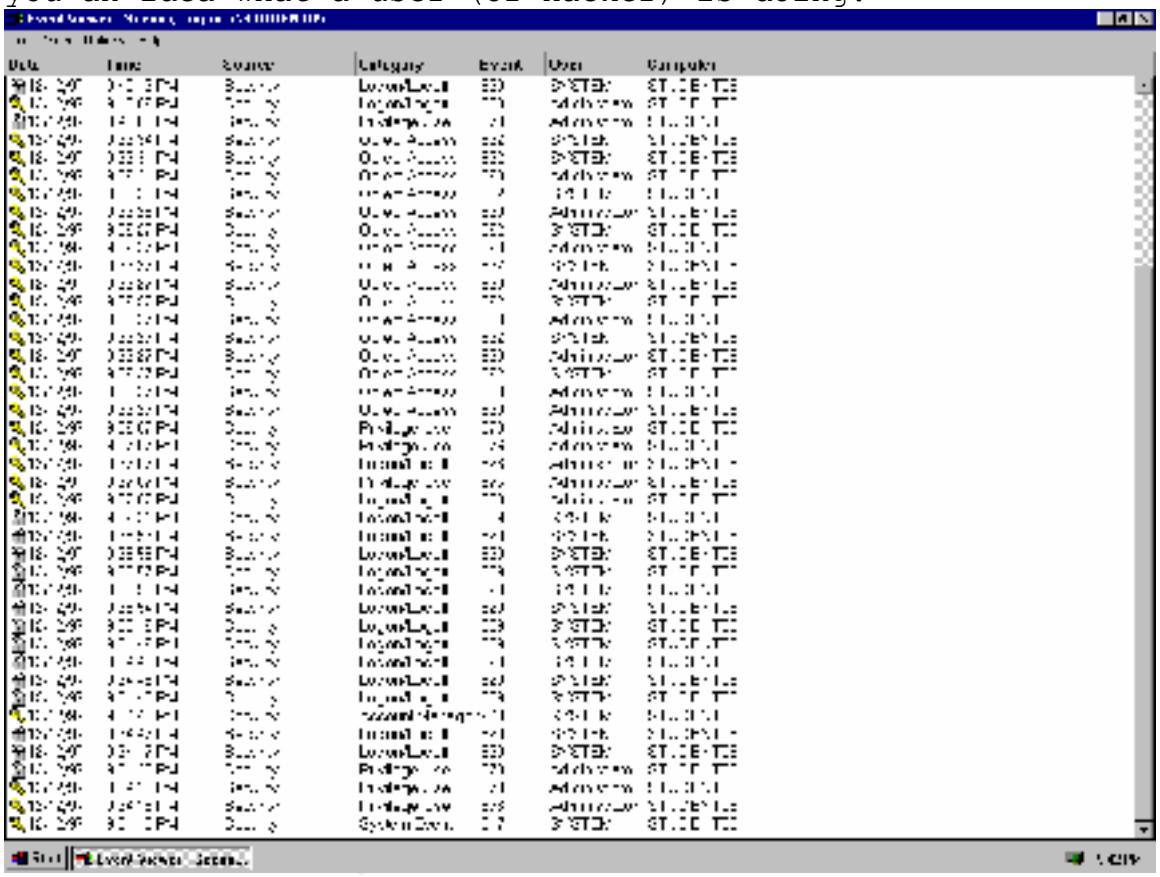
B. We suggest system administrators restore their systems from a clean tape backup to new or

different hard drives. Save the backup tapes and the original hard drives as evidence.

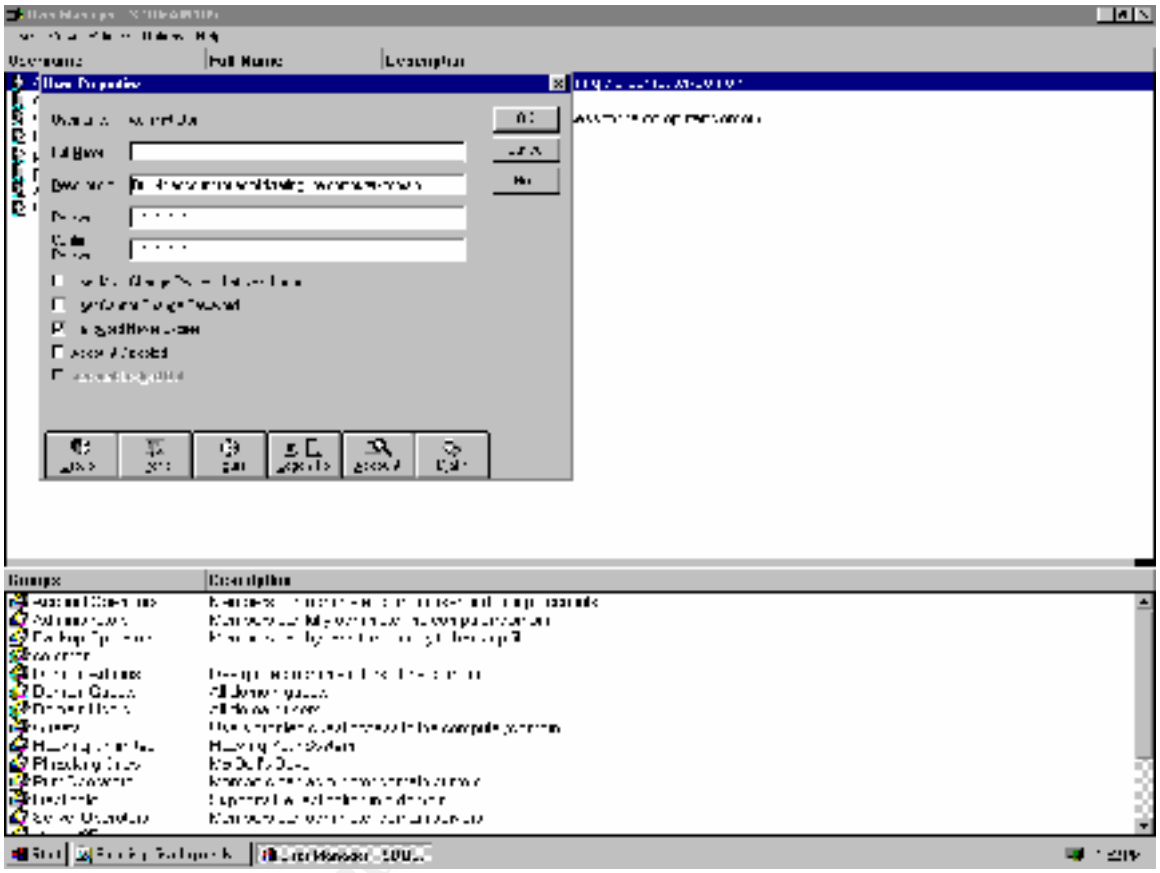
C. Windows NT audit logs policy should be set to monitor most user activity. Failure to set logs will hinder, if not destroy the possibility of a successful conclusion to an incident.



D. If the audit policy is set properly, Windows NT security logs can show a summary of activity and give you an idea what a user (or hacker) is doing.



E. Default passwords must be changed upon installation.



F. System backups should be conducted more frequently. Sysadmins should consider making incremental backups daily.

G. Logging on to a system as root via telnet is a bad idea. Sysadmins must insure that this action is always prohibited.

Appendix 1

TOOL NAME	DESCRIPTION
Adrmpr23	Add/Remove Pro v.2.03 displays the contents of Windows Add/Remove Programs list and checks if each entry is valid. It displays an icon with each entry to show if an entry has a broken link, a link to a missing disk, or a good link. A checker allows the user, himself, to test the validity of the Uninstall String. Add/Remove Pro allows the user to uninstall the selected program or remove the entry from the Windows Add/Remove Programs list.
atrrib-R	Select the Folder where you want to remove the "READ ONLY" attribute from your files. This program comes in handy if you copy a lot of files from CD's to your Hard Drive and need to edit and save files under the same name.
Backup	System backup scheduling utility. Upon running the executable, Backup is run in the background and is accessible from the Windows System Tray.
bdse15	Disk utility for Windows 9x. that allows the PC to read all its hard drives as one big drive; including Jaz, Zip and Syquest. BigDisk's patent-pending technology frees up space that ordinary disk utilities can't. Plus, it's 100% safe.
Bigfixwin	BigFix automatically gathers the latest information about your computer and alerts you. Fixes are automatic, via Fixlet Sites on the Internet.
Byemelis	"Melissa Virus" detection and cleansing utility for MS Office.
c_setup.exe	VectorSoft CPR helps you find special features of Windows 98 that normally are hidden in the user interface. These valuable programs will definitely help you troubleshoot and solve problems, tune-up your system and prevent system errors from occurring.
Cacheman	Cacheman is a utility which tweaks the disk cache settings and prevents frequent swapping of the data to disk resulting in an improved performance and stability.
Clengo23	Clean 'n' Go makes it easy to clean your mouse or keyboard while your computer is on.

core500	A collection of representative utilities from the award-winning Rix2k 5.00 Extreme Power Tools, a package of 60+ Win32 Subsystem 2 (GUI) executables, including 9 tray utilities (CD player, hosts manager, Internet traffic gauge, memory monitor, process manager, task manager, window manager, Winsock utility), 11 editors (animated cursor, icon, 7 text, binary, 2 RTF, direct disk), tray shortcut manager, memory mapper, EXE header viewer, performance stats utility, file system search utility, file date/time stamper, resource monitor, windows command interpreter, drag-drop compliant file comp utility, screen magnifier, bloatware detector, system error utility, admin file access utility and much, much more.
Cpumon	CPU Monitor adds an icon to the Windows 95 System Tray, which shows the current utilization of the systems processor.
ds95.exe	Directory Snoop is a utility program for Windows 95/98 that allows you to snoop around your disk drives at a very low level. Directory Snoop works on any uncompressed FAT12, FAT16, or FAT32 disk.
ezip46.exe	EasyZip brings the convenience of Windows to the use of Zip files. Windows 95, 98, NT, versions included.
Fdlister102	FDL (File and Directory Lister) is a utility for getting a list of your File and Folder names to save and print.
filsnf11	You can tell File Sniffer to look for files which have not been used for a certain number of days. You can specify which folder to look in and whether to include the subfolders when looking for such files. Try File Sniffer, and you might be surprised by the results. Various sorting options are also available to view the results in a desired order. Runs on Windows 95, 98 and NT.
ipc121f.exe	IP Checker version 1.21 shows your local IP-Address with a few, handy options. If you want to copy the address to your Clipboard, just click on the "Copy"-button. Go to the place you want to show the IP-Address, and press Ctrl + V (or find a menu element with the paste function) to paste it into the text.
IPESetup95.exe	InoculateIT Personal Edition protects your computer against viruses, trojans and other malicious software.
lftp13	LeechFTP is a freeware FTP client with some nice features: Multithreading for simultaneous transfers,

	File and Directory Upload, File and Directory Download, URL Connect and URL Download, URL Snatcher (grabs URLs from Clipboard), Sanity check for downloaded ZIP and RAR archives, Archive viewer for ZIP and RAR, Download of directory trees as TAR archives (if supported by server), Queue Timer for scheduled transfers, SmartResume: Aborts resume if files differ, Bandwidth Limiting, FTPSearch Interface, HTTP file download

MMXtest	MMXTest.exe: detects what family of processor you have (8086, 286, 386, 486, Pentium, Pentium pro or Pentium II), detects the presence or absence of MMX processing, tests the MMX instruction set, performs a rough benchmark of your MMX vs. normal compute.
MOBv21.exe	MOB v2 will let you do your backups by either copying all of the data, or zip it onto almost any media. Works with Zip & Jaz Drives, CD-RW, Hard Drives or even Floppy Disks using the Diskspan option.
Partbeta	Ranish Partition Manager, Version 2.38 Beta 1.9 - Hard drive partitioning program
PGPfreeware652a	PGP Freeware brings easy-to-use, strong encryption to the masses. You can use PGP to protect your email, your files, and now even your network connections.
Pingometer1_5.exe	Ping-O-Meter presents ICMP echo and reply data (PINGS) via 2 analog gauge displays as well as 7 digital read outs.
Qcbeta.exe	Q-Copy 2000 is an Explorer shell extension for copying, moving, splitting, zipping and un-zipping files. It provides you with an easy and fast way to deal with file related tasks. Q-Copy 2000 works under Windows 95, Windows 98, Windows NT 4.0 and Windows 2000 RC2.
Rampg1_3	RAMpage is a small Windows utility that displays the amount of available memory in an icon in the System Tray. When the icon is double clicked, the program attempts to free a predefined amount of memory. RAMpage can also be configured to free memory automatically when the amount of available memory drops below a predefined level.
Regb6	Registry Backup 6.0 beta 1 is the latest in the Registry Backup Series. The program runs from DOS to prevent any problems that Windows may create; it detects problems with the registry automatically so it can decide, before Windows boots, as to whether it

	should restore the previous copy of the registry; it's easy to use.
Renamer_12	Utility for renaming one or many files in the same directory folder.
rom2.exe	Revenge of Mozilla II (ROM2) is a utility that removes Internet Explorer from the Windows 98 operating system as well as every other 'Microsoft Internet' component beyond TCP/IP and DUN. In addition, ROM2 also replaces the standard Windows 98 explorer shell with the Windows 95 OSR2 version.
scn2	The Scanner provides a visualization of your media usage. To show the relations optimally, all files and folders of the selected disk(s) are displayed together in one diagram - with an area size proportional to the used space. Smaller objects are invisible, of course. So the Scanner is not intended to be a File Manager.
SetupIPCalc2	IP Subnet Calculator for 32-bit Windows Platforms.

sf_pgr20	The Security Focus Pager is a small utility to keep the user updated on the latest happenings in the computer security industry. It does this by monitoring the Security Focus web site (www.securityfocus.com), and providing a brief description of new content when it is added.
superscan.exe	SuperScan is a TCP port scanner, pinger and hostname resolver, which can perform simple ping tests to tell whether a remote computer is alive, resolve hostnames into IP addresses and reverse lookup IP addresses into hostnames, attempt to connect to other computers on a TCP network to see what services they are running, read responses from connected hosts, scan from a range of addresses and ports.
syscom	SysCom is a tiny "ToolBar"-type program that gives you instant access to all mayor parts of your Win9x-environment: Controls (Input-Devices, System-Setup...), Wizards (Format/Copy, add new hardware...), Tools (Sys-/Regedit...), Folders (Desktop, Network-Neighbourhood, RecicleBin, Templates...), and other stuff (Internet, Audio-CD...).
tc21.exe	TempClean deletes files from your TEMP directories every times you start Windows (or anytime you want) so there is no time for trash to fill up your

	Disk when temporary files have not been deleted by Windows.
treecopy	Have you ever wanted to copy a directory structure without copying the files in Windows? Now you can with TreeCopy. This ingenious program will allow you to select the source directory and destination directory, then it will proceed to copy ONLY the directory structure. This utility is bundled with functionality like selecting Win 9x/NT or Win 3.x display, saving your directory tree to a file and much, much more!
tweakallssetup.exe	TweakAll lets you change many aspects of Windows including (but not limited to) Startup and Shutdown Logos, support for 3dfx Voodoo 1, 2, 3 and Banshee video cards, image quality settings and also overclock your card for more performance, tighten up the security on your system on a per user basis, gain control over Windows hard drive and CD-ROM caches, speed up your internet connection, and too much more to mention here!
w95krnltoys.exe	The Windows 95 kernel team got kind of jealous of all the attention the shell team has been getting from its PowerToys, so they decided to polish off their own personal toys and make their own web page. Mind you, the kernel folks aren't experts at intuitive user interfaces, so don't expect to see jumping icons and friendly things to click on. (These are the people who do their taxes in hexadecimal.)

whois104.exe	If you've got *any* sort of trouble with an Internet domain, "Whois" is useful. It indicates if the domain actually exists, the people or organization behind it and often gives their alternative contact details. It's useful for more advanced spam tracking but it's handy in its own right.
wt98_40.exe	WinTune 98 is a low-level benchmark test suite that tests the performance of the major systems of a PC running Windows 95, Windows 98, or Windows NT.
wxi9x-30	Win-eXpose-I/O for Windows 95,98 is a file I/O Tracing/Debugging SHAREWARE windows util. that lets you examine in real time what files each running application is using or trying to use.
xclone13	XCLONE is a disk/directory copying tool that easily lets you duplicate entire disks or directory trees. I primarily use it to move operating systems when

	upgrading to a larger hard drive. It is also useful for backing up to another hard drive or saving programs before installing a new version.