CERT® Coordination Center and AusCERT

Windows Intruder Detection Checklist

This document is being published jointly by the CERT Coordination Center and AusCERT (Australian Computer Emergency Response Team).

printable version

A. Introduction
B. General Advice Pertaining to Intrusion Detection
C. Look for Signs that Your System may have been Compromised
   1. A Word on Rootkits
   2. Examine Log Files
   3. Check for Odd User Accounts and Groups
   4. Check All Groups for Unexpected User Membership
   5. Look for Unauthorized User Rights
   6. Check for Unauthorized Applications Starting Automatically
   7. Check Your System Binaries for Alterations
   8. Check Your Network Configurations for Unauthorized Entries
   9. Check for Unauthorized Shares
   10. Check for Any Jobs Scheduled to Run
   11. Check for Unauthorized Processes
   12. Look Throughout the System for Unusual or Hidden Files
   13. Check for Altered Permissions on Files or Registry Keys
   14. Check for Changes in User or Computer Policies
   15. Ensure the System has not been Joined to a Different Domain
   16. Audit for Intrusion Detection
   17. Additional Information
D. Consider Running Intrusion Detection Systems If Possible
   1. Freeware/shareware Intrusion Detection Systems
   2. Commercial Intrusion Detection Systems
E. Review Other AusCERT and CERT Documents
   1. Steps for Recovering from a Windows NT Compromise
   2. Windows NT Configuration Guidelines
   3. NIST Checklists
F. Document Revision History

A. Introduction

This document outlines suggested steps for determining whether your Windows system has been compromised. System administrators can use this information to look for several types of break-ins. We also encourage you to review all sections of this document and modify your systems to address potential weaknesses.

The term "Windows system" is used throughout this document to refer to systems running Windows 2000, Windows XP, and Windows Server 2003. Where there is a distinction between the various operating system versions (e.g., a capability available to only one OS version) the document will note this as such.

In this document, we make a distinction between the terms "auditing" and "monitoring". We use auditing to indicate the logging or collection of information and use monitoring to indicate the routine review of information obtained by auditing to determine occurrences of specific events.

This document does not provide intrusion detection methods for Windows 9x (including Windows ME). These operating systems lack the underlying subsystems necessary to secure them and should not be used in a commercial environment or on workstations where data is considered critical.

This document will be most useful to you if you have some familiarity with Windows operating systems and also have the following prerequisite knowledge:

- Knowledge of how to execute commands in the context of LocalSystem
- Familiarity with the Windows filesystems (particularly NTFS)

- Familiarity with the Windows Registry
- Knowledge of Windows systems administration

The following conventions are used to refer to registry hives:

HKCR	HKEY_CLASSES_ROOT
HKLM	HKEY_LOCAL_MACHINE
HKU	HKEY_USERS
HKCU	HKEY_CURRENT_USER
HKCC	HKEY_CURRENT_CONFIG

B. General Advice Pertaining to Intrusion Detection

Proactive auditing and monitoring are essential steps in intrusion detection. It is ineffective to audit altered data or compromised systems -- their logs are unreliable. Establish a baseline for what you consider normal activity for your environment so you can determine unusual events and respond appropriately. See section C16 of this document for more information on audit settings and events useful to detect successful attacks or attacks in progress.

When searching for signs of intrusion, examine all machines on the local network. Most of the time, if one host has been compromised, others on the network have also been compromised.

We also encourage you to regularly check with your vendor(s) for any updates or new patches that relate to your systems.

Note: All actions taken during the course of an investigation should be in accordance with your organization's policies and procedures. At the very least, follow these steps before you start analyzing a system you suspect has been compromised:

- Document every step that you perform in detail.
- Perform a sector-by-sector backup of the hard disk drive.
- If your organization intends to take legal action in connection with intrusions, then consult with your legal department before performing any step.

C. Look for Signs that Your System May Have Been Compromised

1. A Word on Rootkits

Rootkits have become prevalent on Windows platforms. Unfortunately, they are freely available and increasingly easy to use. A rootkit is software much like a Trojan horse, typically designed to perform a number of tasks. A rootkit can

- hide its existence and therefore the fact that the system has been compromised.
- capture information such as user passwords.
- install backdoors which can be used for remote access by malicious individuals.
- allow the affected machine to be used as a staging point for further exploitation and to attack and compromise other systems.

The following are some products which may assist in rootkit detection. These tools may require "SYSTEM" privileges in order to properly access certain parts of the operating system needed to detect rootkits. Some rootkits may not be detectable while the infected OS is running. To detect these rootkits, it is important that you run your detection utility from a clean OS.

Note: Some of these programs may cause system instability or system corruption; test them in an isolated environment before using them in production.

- Rkdetect, available from http://www.security.nnov.ru/soft/
- RootKit Revealer, available from http://www.sysinternals.com/Utilities/RootkitRevealer.html

- VICE, a hooker detection tool, available from http://www.rootkit.com (registration required)
- BartPE, a bootable CD-based OS capable of running Win32 binaries: http://www.nu2.ne/pebuilder/
- WinPE, which is similar to BartPE, however there is no GUI support. See http://www.microsoft.com/licensing/programs/sa/support/winpe.mspx for availability information.

2. **Examine log files**

   Examine log files for connections from unusual locations or for other unusual activity. You can use the Event Viewer to check for odd logon entries, failures of services, or unexplained system restarts. If your firewall, web server, or router writes logs to a location different than the system being investigated, remember to check these logs as well. Remember, this is not foolproof unless you log to append-only media or a secure logging server; many intruders edit or remove log files in an attempt to hide their activity.

3. **Check for odd user accounts and groups**

   You can use "Local Users and Groups" (lusrmgr.msc) from a domain member or stand alone computer or the "net user", "net group" and "net localgroup" commands at the command line. One other option is to use the "wmic useraccount" command. On a domain controller, "Active Directory Users and Computers" (dsa.msc) may be used to view and verify domain accounts, however "net user" and "net group" will still work.

4. **Check all groups for unexpected user membership**

   Some of the built-in groups give special privileges to the members of those groups. For example, members of the Administrators group can do anything to the local system. Backup operators can read any file on the system. Power Users can create shares. Users with Debug privileges should be considered equal to Administrator accounts.

5. **Look for unauthorized user rights**

   To examine user rights, use the User Manager tool under Policies, User Rights. There are 28 different rights that can be assigned to users or groups. Generally, the default configuration for these rights is secure. One right to take note of is the "SeDebugPrivilege." This right allows a user to connect a debugger to any process, including the kernel. Information regarding the default privileges assigned to user accounts for Windows XP can be found here:

   http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prnd_urs_mhnn.asp

   You can also check (or modify) user privileges using ntrights.exe from the Windows Server 2003 Resource Kit.

6. **Check for unauthorized applications starting automatically**

   There are a number of methods an intruder could use to start a backdoor program, so be sure to check the Startup folders. Check all items in "C:\Documents and Settings\%username%\Start Menu\Programs\Startup" folders (for Windows NT4, Substitute "C:\Documents and Settings" for "C:\WINNT40\Profiles"). You can also examine all the shortcuts by selecting Start, Programs, and Startup. Note that there are two startup folders, one for the local user and one for all users. When a user logs on, all of the applications in both the "All Users" and in the user's startup folder are started. This makes it important to check all of the startup folders for suspicious applications.

   Check the registry. The most common locations for applications to start through the registry are:

   - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup

- HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows
- HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs
- HKLM\System\ControlSet001\Control\Session Manager\KnownDLLs
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load
- HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows

Check for unauthorized services. Some backdoor programs will install themselves as a service that is started when the system boots up. Services can then run as any user with the "Logon as a Service" user right. Check services that are started automatically and be sure that they are necessary. Also, check that the service executable file is not a Trojan horse or a backdoor program.

The following command will output information regarding installed services to a formatted html file:

```
wmic /output:C:\services.htm service get /format:hform
```

This command will work on Windows XP or later, but will not operate if run directly from a Windows 2000 or NT machine. Additionally, this command can be used from a Windows XP machine to enumerate services on any machine which uses WMI (available on Windows NT4 SP4 and later).

For further information regarding WMI and the WMI Command Line tool (WMIC), see the following document:

Windows Management Instrumentation Command-line:

- http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/WMIC_info.asp

Check legacy files such as Autoexec.bat, Autoexec.nt, config.sys, system.ini and win.ini for unauthorized changes. These files can be used to start programs when the machine boots.

- Sysinternals Autoruns is a freeware utility that displays the contents of auto-run locations.

7. **Check your system binaries for alterations**

Compare the versions on your systems with copies that you know have not been altered, such as those from your initial installation media. Be cautious of trusting backups; they could also contain malicious software (malware).

Trojan horse programs may produce the same file size and timestamp as the legitimate version. Therefore, just checking file properties and timestamps associated with the programs is not sufficient for determining whether the programs have been replaced. Instead, use an MD5 or SHA-1 checksum generation/validation utility such as WinMD5Sum, Microsoft's File Checksum Integrity Verifier, Sysinternals sigcheck, Microsoft LogParser, a host-based IDS such as GFI LanSIM , or other cryptographic checksum tools such as Tripwire to detect these trojan horse programs, (provided that the checksum tools themselves are kept secure and are not available for modification by the intruder). You may also want to consider using a tool, such as PGP, to cryptographically sign the output generated by WinMD5Sum or LanSIM so that it can be used for future reference.

Windows XP also includes a component called "Windows File Protection" (WFP). WFP monitors critical system files for changes and replacements. WFP uses file signatures and catalogue files generated by code signing to determine if protected files have been modified.

The replacement of protected system files is supported using a limited number of methods:

- Windows Service Pack installation using Update.exe
- Hotfixes installed using Hotfix.exe or Update.exe
- Operating system upgrades using Winnt32.exe
- Windows Update
- WFP provides a utility called System File Checker (sfc.exe) to manage Windows File Protection

For further information on Windows File Protection see the following documents:

- Description of the Windows File Protection Feature
  http://support.microsoft.com/?kbid=222193

- Description of Windows XP and Windows Server 2003 System File Checker (Sfc.exe)
  http://support.microsoft.com/?kbid=310747

- Windows File Protection Registry Settings
  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wfp/setup/wfp_registry_values.asp

Using anti-virus and spyware detection software will also help you check for computer viruses, backdoors, and Trojan horse programs. Remember that people are always creating new malicious programs, so it is important to keep these software packages up to date.

8. **Check your network configuration for unauthorized entries**

Look for invalid entries for settings such as WINS, DNS, IP forwarding, and the like. These settings can be checked using the Network Properties tool or using the "ipconfig /all" command at the command prompt. As an additional measure, the Port Reporter tool from Microsoft is quite useful for monitoring applications which open ports for inbound and outbound connections.

The Port Reporter tool and a log parser are available from Microsoft:
http://support.microsoft.com/?kbid=837243

Make sure that only the network services you want to have running on your system are listed in the Network Services configuration. Additionally, check your hosts file, located under %systemroot%\system32\drivers\etc\hosts for unauthorized entries. Check for odd ports listening for connections from other hosts by using the "netstat -an" command. The following batch file parses ports that are in a listening or connected state. Fport from Foundstone Inc. will attempt to map ports to the services listening on them.

```
@echo off
netstat -an > gports
find "LISTENING" < gports > oports.txt
find "ESTABLISHED" < gports >> oports.txt
del gports
```

Windows XP enables you to view the process which "owns" a particular port using "netstat -ao". Note that this will only show the Process ID of the owning process. Users with XP Service Pack 2 can use the "-b" or "-vb" netstat options. The "-b" option will show the executable that corresponds to the Process ID owning the port. The "-vb" option will also include the components that were used to create the port or connection. To convert the Process ID's discovered using the "-ao" option into their process names, use the following command :

```
wmic process where ProcessId='x' get caption
```

Note: In this instance, 'x' is used to indicate any valid process ID identified in the previous step.

Windows XP SP2 and Windows 2003 SP1 include a netsh command to list Layered Service Providers installed on a machine. Layered Service Providers have the ability to access all data received and sent by a machine. They also have the ability to manipulate the data. Layered Service Providers may provide enhancements for communications but can also be used for malicious activity. To check for Layered Service Providers that have been installed, execute the following commands on the command prompt:

```
netsh winsock show catalog
```

See the following documents for a list of commonly used port numbers:

- IANA port assignments
  http://www.iana.org/assignments/port-numbers

- Windows 2000 TCP and UDP port assignments
  http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/tcpip/part4/tcpappc.mspx

Additional ports used by Microsoft products can be found in the following Microsoft Knowledgebase articles:

- Port requirements for the Microsoft Windows Server System http://support.microsoft.com/?kbid=832017

- Microsoft Exchange 2003 assigns ports to services dynamically at service startup, see the following article for further information.
http://support.microsoft.com/?kbid=833799

- Ports that Systems Management Server 2003 uses to communicate through a firewall or proxy server
http://support.microsoft.com/?kbid=826852

- Ports used in Server 2003 Trust Relationships
http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR_trust_tools.asp

9. **Check for unauthorized shares**

You can use the "net share" command at the command prompt or use the Server Manager tool to list all the shares on a system. Windows systems provide a way to create hidden shares by adding a '$' to the end of a share name.

There are a few default share names that Windows uses (such as PRINT$), but if you are not sharing a printer with other users, check to see why that share was created. By default, the root of each drive is shared as an "Administrative Share" (e.g., C$). This is typically used by Domain Administrators for management of remote machines. To view shares on a local or remote machine, use Shared Folders Management (fsmgmt.msc). If you notice an odd share name, the aforementioned tool will show you the actual location on the system that is being shared. A drive or directory can have multiple share names, each with possibly different permissions associated with them.

The following are the default administrative shares:

DriveLetter$	Root partitions and volumes
Admin$	%SYSTEMROOT%
IPC$	Named pipes
NETLOGON	Used for domain controllers
SYSVOL	Used for domain controllers
Print$	Printer
FAX$	Fax

Note: Some of these may not be on a user's system depending on configuration.

10. **Check for any jobs scheduled to run**

Intruders can leave back doors in files that are scheduled to run at a future time. This technique can let an intruder back on the system (even after you believe you had addressed the original compromise). Verify that all files and programs referenced (directly or indirectly) by the scheduler and the job files themselves are not world-writable. To check for jobs currently pending, use the "at" command, "schtasks" command or the Windows Task Scheduler.

11. **Check for unauthorized processes**

You can use the Task Manager tool or the pulist.exe and tlist.exe commands from the Windows resource kit at the command prompt to gather information about the processes running on your system. Another good tool for getting this information is Process Explorer from Sysinternals. A number of shareware/freeware applications such as Filemon from

Sysinternals also exist to show what files are in use. Regmon from Sysinternals is also useful to check in real time which applications are accessing the registry and what actions they are taking.

With the pulist.exe command, you can see who started each process. Services are usually associated with the SYSTEM account. Check to see that services are not running with elevated privileges. Also, you should check for abnormal account names. The tlist.exe command with the -t flag will show you which processes started child processes. Additionally, Windows XP and Server 2003 include the tasklist.exe command which, when used with the /svc switch, allows viewing of processes running under "svchost.exe", and when used the /m switch, allows viewing of all loaded modules.

Microsoft has also provided the System Information tool which gives information about other areas of interest, including:

- Running Tasks
- Loaded Modules
- Services
- Startup Programs
- Drivers

The System Information tool can be invoked by running msinfo32.msc from a command prompt.

12. **Look throughout the system for unusual or hidden files**

Unusual or hidden files can be used to hide tools and information such as password cracking programs, password files from other systems, and the like. Hidden files can often be found and viewed with Explorer. To do so, Select "Tools, Folder Options, View," then select "Show hidden files and folders". After that, deselect "Hide file extensions for known file types" and "Hide protected operating system files". To view hidden files at the command prompt, type 'dir /ah.' On the NTFS file system it is possible to hide data in alternate data streams. Sysinternals Streams utility can be used to search for alternate data streams.

Note: Running as LocalSystem or booting from a CD-based OS such as Knoppix or BartPE/WinPE will enable viewing of files in protected directories and may show those hidden by rootkits.

13. **Check for altered permissions on files or registry keys**

Part of properly securing a Windows system is to limit permissions on files and registry keys so that unauthorized users cannot start unauthorized programs (e.g., backdoors or keyloggers) or change system files. In order to check many files throughout your directory tree, you can use the xcacls.exe or showacls.exe programs that are part of the Resource Kit.

It is important to create a baseline of file and registry permissions for comparisons after the initial installation and setup. The Local Security Settings console (secpol.msc) can also be used to analyze your system against a configuration you have defined previously. This would help to determine what may have been modified.

14. **Check for changes in user or computer policies**

Policies are used on Windows systems to define a wide variety of configurations and can be used to control what users can and cannot do. For standalone or workgroup machines, these policies are configured via the Local Computer Policy. In an Active Directory domain, these options are typically configured using Group Policy on a Domain Controller, then linked to an Organizational Unit.

We recommended you keep a current copy of the policies you create in case they are altered and you need to determine what was changed. You can use the "gpresult /v" command to see what current Group Policy Objects have been applied and their settings. Microsoft also offers GPInventory to allow administrators to collect multiple Resultant Sets of User Policy along with some other information.

15. **Ensure the system has not been joined to a different domain**

An intruder may attempt to gain Domain Administrator access to a workstation by changing the current domain to a domain that the intruder controls.

16. **Audit for intrusion detection**

The following tables list available auditing options for Windows, recommended settings for auditing, and examples of events which may indicate an in-progress or successful attack.

To enable auditing on a stand-alone or workgroup machine, run gpedit.msc from a command line. In a domain environment, you can use Active Directory Users and Computers (dsa.msc), or GPMC.msc (Group Policy Management Console). For more information regarding this tool, see the following document:

Administering Group Policy with the GPMC
http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

The following table lists available auditing options, their meanings and recommended settings:

Audit option	Setting	Purpose
Audit System Events	Success/Failure	Events are logged when a user or process alters aspects of the computer environment, such as a startup or shutdown.
Audit Logon Events	Success/Failure	Logs local user and computer logon successes and failures; for example Event ID 528 indicates a successful logon to the computer. Event ID 529 indicates a failed logon.
Account Logon Events	Success/Failure	Audits Domain user and computer logons, note that when a user attempts to logon to the domain, the event will be recorded only by the logon server which handled the request
Account Management	Success/Failure	Records additions, deletions, and modifications of users and local groups (when enabled on a domain member) or domain users/groups, (when enabled on a domain controller)
Audit Object Access	Success/Failure	Enables auditing of any object with a SACL (System Access Control List); e.g., folders, files, printers, registry keys, and the like. It should be noted that auditing object access will simply allow objects to be configured for auditing. You will need to configure auditing for an object on the object itself.

The following Table lists commonly monitored events which may indicate successful attacks or attacks in process on your systems. Each of these events are logged to the Security event log.

Event ID	Indication	Audit Policy Required
528	Successful user logon	Audit Logon Events (Success)
529	Unknown user or bad password	Audit Logon Events (Failure)
530	Logon attempt outside of allowed hours	Audit Logon Events (Failure)

531	Account currently disabled	Audit Logon Events (Failure)
532	The specified user account has expired.	Audit Logon Events (Failure)
533	User not allowed to logon to this computer	Audit Logon Events (Failure)
534	The user has not been granted the requested logon type at this computer.	Audit Logon Events (Failure)
537	Unexpected error during logon	Audit Logon Events (Failure)
539	Account locked out	Audit Logon Events (Failure)
540	Successful network logon	Audit Logon Events (Success)
560	Access was granted to an already existing object.	Audit Object Access (Success)
563	An attempt was made to open an object with the intent to delete it.	Audit Object Access (Success)
564	A protected object was deleted.	Audit Object Access (Success)
577	Indicates that a user has attempted to perform a privileged operation	Audit Privilege Use
577 (SeShutdownPrivilege)	Indicates an system shutdown attempt	Audit Privilege Use
577/578 (SeTcbPrivilege)	Act as part of the operating system. (This right should not be assigned to any user account.)	Audit Privilege Use
577/578 (SeSystemtimePrivilege)	Shows an attempt to change the system time	Audit Privilege Use
577/578 (SeLoadDriverPrivilege)	Indicates an attempt to load or unload a device driver	Audit Privilege Use

577/578 (SeSecurityPrivilege)	Indicates an attempt to clear the event log or write privilege use events	Audit Privilege Use
577/578 (SeTakeOwnershipPrivilege)	Indicates that a user has attempted to take ownership of an object	Audit Privilege Use
624	User Account Created	Audit Account Management (Success)
625	User account type changed	Audit Account Management (Success)
626	User account enabled	Audit Account Management (Success)
627	Password Change Attempted	Audit Account Management (Failure)
632	Security Enabled Global Group Member Added	Audit Account Management (Success)
633	Security Enabled Global Group Member Removed	Audit Account Management (Success)
636	Security Enabled Local Group Member Added	Audit Account Management (Success)
644	User Account Locked Out	Audit Account Management (Failure)
675	Kerberos pre-authentication failed	Audit Account Logon Events (Failure)
677	A TGS ticket was not granted (indicates failed domain logon attempt).	Audit Account Logon Events (Failure)
682	User has reconnected a terminal services session	Audit Logon Events (Success)

Monitor events which will assist you in identifying and responding to intrusion attempts on your network. For example, a brute force attack on an account will typically generate a large number of "Unknown username or bad password" events (Event ID 529).

The following documents describe how to enable auditing for a Windows Domain, and provide further information regarding interpretation of the events generated by auditing:

Windows 2000:
http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/09detect.mspx

Windows 2003:
http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_SEprocsAuditing.asp

It is important to note that logging may not occur on all machines within a domain. For example, a logon attempt will only be recorded on the logon server which processed the request and not on all logon servers in a domain, so event log collation is necessary to monitor your auditing. There are several freeware and commercial tools which can be useful for this process:

EventCombMT, included in the Windows Server 2003 Resource Kit, is a tool for parsing event logs on multiple systems simultaneously.

Dumpel, included in the Windows 2000 Resource Kit Tools, is a command line tool to dump local or remote event logs to a tab or comma-separated file and is capable of filtering events.

Scripting can also be used to retrieve events from event logs. Microsoft even offers sample scripts which can be customized to suit your needs.

You should also periodically review any log files residing in %systemroot%\system32\logfiles. By default IIS will log to this directory as will other applications.

To assist with the retrieval of useful data from these logs, take a look at LogParser available from:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=8cde4028-e247-45be-bab9-ac851fc166a4

17. **Additional Information**

The Technet Security Resource Center provides a wealth of information regarding computer and information security including how-to's and guides to best practices. The Technet Security Resource Center can be found here:
http://www.microsoft.com/technet/security/default.mspx

The Windows XP Security Guide:
http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en

D. Consider Running Intrusion Detection Systems if Possible

1. Freeware/shareware Intrusion Detection Systems

- The COAST Intrusion Detection System Resources web page has a list of some freeware/shareware intrusion detection systems.
  http://www.cerias.purdue.edu/coast/ids/

- GFI System Integrity Monitor
  http://www.gfi.com/downloads/downloads.asp?pid=9&vid=1&lid=1

2. Commercial Intrusion Detection Systems

- Tripwire
  http://www.tripwire.com

- Real Secure Server Sensor
  http://www.iss.net/products_services/enterprise_protection/rsserver/protector_server.php

- eEye SecureIIS
  http://www.eeye.com/html/products/secureiis/

- Intact

http://pedestalsoftware.com/products/

Please note that the provision of links to these products does not indicate endorsement of these products by the CERT/CC.

E. Review Other AusCERT and CERT Documents

1. Steps for Recovering from a UNIX or NT System Compromise
   http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

2. Windows NT Configuration Guidelines
   http://www.auscert.org.au/1970

3. NIST Checklists and information guides relating to secure configuration of various applications, devices and systems:
   http://csrc.nist.gov/pcig/cig.html

F. Document Revision History

Initial Release: April 17, 2000

Updated for Windows 2000/XP: January 17, 2006

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

https://www.cert.org/pgp/cert_pgp_key.asc

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information