Unusual Log Entries

To look at logs, run the Windows event viewer:

```
C:\> eventvwr.msc
```

Or, invoke the event viewer by going to:

Start→Programs→Administrative Tools→Event Viewer

Look for suspicious events, such as:

- “Event log service was stopped.”
- “Windows File Protection is not active on this system.”
- "The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..."
- “The MS Telnet Service has started successfully.”
- Look for large number of failed logon attempts or locked out accounts.

Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager → Process and Performance tabs

Look for unusual system crashes, beyond the normal level for the given system.

Additional Supporting Tools

The following tools are not built into the Windows operating system, but can be used to analyze its security status in more detail. Each is available for free download at the listed web site.

DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.

Tools for mapping listening TCP/UDP ports to the program listening on those ports:

Fport – command-line tool at www.foundstone.com

TCPView – GUI tool at www.microsoft.com/technet/sysinternals

Process analysis tools from the Windows 2000 Resource Kit -- http://support.microsoft.com/kb/927229:

- pulist – shows user name associated with each running process
- pstat – shows detailed process statistics, including name, Pid, memory, etc.

Additional Process Analysis Tools:

- Process Explorer – GUI tool at www.microsoft.com/technet/sysinternals
- TaskMan+ -- GUI tool at http://www.diamondcs.com.au

The Center for Internet Security has released various Windows security templates and security scoring tools for free at www.cisecurity.org.

Intrusion Discovery

Cheat Sheet v2.0

Windows 2000

POCKET REFERENCE GUIDE

SANS Institute

http://www.sans.org

http://isc.sans.org

Download the latest version of this sheet from http://www.sans.org/resources/win2ksacheatsheet.pdf

Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

How To Use This Sheet

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Unusual Processes and Services
- Unusual Files and Reg Keys
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

If you spot anomalous behavior: **DO NOT PANIC!** Your system may or may not have come under attack. Please contact the Incident Handling Team immediately to report the activities and get further assistance.

Unusual Processes and Services

Look for unusual/unexpected processes by running Task Manager:
(Start→Run… and type `taskmgr.exe`)

Look for unusual network services installed:

```
      C:\> net start
```

Look for unusual started network services (GUI):

```
      C:\> services.msc
```

You need to be familiar with the normal processes on the machine and search for deviations from the norm.

Unusual Files and Registry Keys

Check file space usage to look for sudden major decreases in free space, using the GUI (right-click on partition), or type:

```
      C:\> dir c:\
```

Look for unusually big files: Start→Search→For Files of Folders… Search Options→Size→At Least 10000KB

Look for strange programs referred to in registry keys associated with system start up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

To check the registry, run:

```
      C:\> regedit.exe
```

Unusual Network Usage

Look at file shares, and make sure each has a defined business purpose:

```
C:\> net view \\127.0.0.1
```

Look at who has an open session with the machine:

```
C:\> net session
```

Look at which sessions this machine has opened with other systems:

```
C:\> net use
```

Look at NetBIOS over TCP/IP activity:

```
C:\> nbtstat –S
```

Look for unusual listening TCP and UDP ports:

```
C:\> netstat –na
```

For continuously updated and scrolling output of this command every 5 seconds:

```
C:\> netstat –na 5
```

Windows XP and 2003 include the –o flag for showing owning process id:

```
C:\> netstat –nao 5
```

Again, you need to understand normal port usage for the system and look for deviations.

Unusual Scheduled Tasks

Look at scheduled tasks on the local host by running:

```
      C:\> at
```

Also, check the scheduled tasks using the Task Manager, invoked by going to:
Start→Programs→Accessories→System Tools→Scheduled Tasks

Look for unusual scheduled tasks, especially those that run as a user in the Administrator's group, as SYSTEM, or with a blank user name.

Look for unexpected entries in user autostart directories:

- C:\Documents and Settings\[user_name]\Start Menu\Programs\StartUp
- C:\Winnt\Profiles\[user_name]\Start Menu\Programs\StartUp

Unusual Accounts

Look for new, unexpected accounts in the Administrators group:

```
C:\> lusrmgr.msc
```

Click on Groups, Double Click on Administrators, then check members of this group.

This can also be done at the command prompt:

```
C:\> net user

C:\> net localgroup administrators
```