Unusual Log Entries

Check your logs 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.

To do this using the GUI, run the Windows event viewer:

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

Using the command prompt:

```
      C:\> eventquery.vbs | more
```

Or, to focus on a particular event log:

```
      C:\> eventquery.vbs /L security
```

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 Windows operating system but can be used to analyze security issues 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

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.

SANS INSTITUTE

Intrusion Discovery

Cheat Sheet v2.0

Windows XP Pro / 2003 Server / Vista

POCKET REFERENCE GUIDE

SANS Institute

www.sans.org and isc.sans.org

Download the latest version of this sheet from http://www.sans.org/resources/winsacheatsheet.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, and focus on processes with User Name “SYSTEM” or “Administrator” (or users in the Administrators' group). You need to be familiar with normal processes and services and search for deviations.

Using the GUI, run Task Manager:

```
        C:\> taskmgr.exe
```

Using the command prompt:

```
        C:\> tasklist
        C:\> wmic process list full
```

Also look for unusual services.

Using the GUI:

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

Using the command prompt:

```
        C:\> net start
        C:\> sc query
```

For a list of services associated with each process:

```
        C:\> tasklist /svc
```

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

Note that you should also check the HKCU counterparts (replace HKLM with HKCU above).

Using the GUI:

```
        C:\> regedit
```

Using the command prompt:

```
        C:\> reg query <reg key>
```

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
```

The –o flag shows the owning process id:

```
        C:\> netstat –nao 5
```

The –b flag shows the executable name and the DLLs loaded for the network connection.

```
        C:\> netstat –naob 5
```

Note that the –b flag uses excessive CPU resources.

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

Also check Windows Firewall configuration:

```
        C:\> netsh firewall show config
```

Unusual Scheduled Tasks

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

Using the GUI, run Task Scheduler: Start→Programs→Accessories→System Tools→Scheduled Tasks

Using the command prompt:

```
        C:\> schtasks
```

Check other autostart items as well for unexpected entries, remembering to check user autostart directories and registry keys.

Using the GUI, run msconfig and look at the Startup tab:

Start → Run, **msconfig.exe**

Using the command prompt:

```
        C:\> wmic startup list full
```

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
```