Unusual Log Entries

To look at logs, run event viewer:

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

Look for suspicious events:

"Event log service was stopped."

"Windows File Protection is not active on this system."

"The MS Telnet Service has started successfully."

Look for large number of failed logon attempts or locked out accounts.

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.

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

Fport (www.foundstone.com)

TCPView (www.sysinternals.com)

File integrity checking tools – Osiris (http://osiris.shmoo.com/download.html)

Windows 2000 Resource Kit Tools (http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp)

Especially pulist and pstat

pulist and pstat which show detailed information about running processes

Intrusion Discovery

Cheat Sheet

Windows 2000/XP

POCKET REFERENCE GUIDE

SANS Institute
incidents@sans.org
+1 317.580.9756
http://www.sans.org
http://www.incidents.org

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.

What to use this sheet for

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
- Unusual Files
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- 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:

[Chief Handler's Name]
[Contact Phone Number]
[Contact Pager Number]
[Relevant Internal Web Site]

Unusual Processes

Look for unusual/unexpected processes:

Run Task Manager
(Start→Run… and type `taskmgr.exe`)

On Windows XP and 2003, focus on processes with User Name "SYSTEM" or "Administrator"
(or users in the Administrator's group)

Look for unusual network services:
`C:\> net start`

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

Unusual Files

Check file space usage to look for sudden major decreases in free space

Use 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 10000 KB

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:
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

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