



Interested in learning
more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

SCORE Security Checklist

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
```



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced