



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 Accounts

Look in /etc/passwd for new accounts in sorted list by UID:

```
# sort -nk3 -t: /etc/passwd | less
```

Normal accounts will be there, but look for new, unexpected accounts, especially with UID < 500.

Also, look for unexpected UID 0 accounts:

```
# egrep ':0+:' /etc/passwd
```

On systems that use multiple authentication methods:

```
# getent passwd | egrep ':0+:'
```

Look for orphaned files, which could be a sign of an attacker's temporary account that has been deleted.

```
# find / -nouser -print
```

## Unusual Log Entries

Look through your system log files for suspicious events, including:

- "entered promiscuous mode"
- Large number of authentication or login failures from either local or remote access tools (e.g., telnetd, sshd, etc.)
- Remote Procedure Call (rpc) programs with a log entry that includes a large number (> 20) strange characters (such as ^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)
- For systems running web servers: Larger than normal number of Apache logs saying "error"
- Reboots and/or application restarts

## Other Unusual Items

Sluggish system performance:

```
$ uptime - Look at "load average"
```

Excessive memory use: \$ free

Sudden decreases in available disk space:

```
$ df
```

## Additional Supporting Tools

The following tools are often not built into the Linux 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.**

Chkrootkit looks for anomalies on systems introduced by user-mode and kernel-mode RootKits – [www.chkrootkit.org](http://www.chkrootkit.org)

Tripwire looks for changes to critical system files – [www.tripwire.org](http://www.tripwire.org) - free for Linux for non-commercial use

AIDE looks for changes to critical system files <http://www.cs.tut.fi/~rammer/aide.html>

The Center for Internet Security has released a Linux hardening guide for free at [www.cisecurity.org](http://www.cisecurity.org).

The free Bastille Script provides automated security hardening for Linux systems, available at [www.bastille-linux.org](http://www.bastille-linux.org).



## Intrusion Discovery

### Cheat Sheet v2.0

Linux

POCKET REFERENCE GUIDE

SANS Institute

[www.sans.org](http://www.sans.org) and [isc.sans.org](http://isc.sans.org)

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

## 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 and Services
- Unusual Files
- 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 at all running processes:

```
# ps -aux
```

Get familiar with "normal" processes for the machine. Look for unusual processes. Focus on processes with root (UID 0) privileges.

If you spot a process that is unfamiliar, investigate in more detail using:

```
# lsof -p [pid]
```

This command shows all files and ports used by the running process.

If your machine has it installed, run chkconfig to see which services are enabled at various runlevels:

```
# chkconfig --list
```

## Unusual Files

Look for unusual SUID root files:

```
# find / -uid 0 -perm -4000 -print
```

This requires knowledge of normal SUID files.

Look for unusual large files (greater than 10 MegaBytes):

```
# find / -size +10000k -print
```

This requires knowledge of normal large files.

Look for files named with dots and spaces ("...", ".. ", ". ", and " ") used to camouflage files:

```
# find / -name " " -print
# find / -name ".. " -print
# find / -name ". " -print
# find / -name " " -print
```

## Unusual Files Continued

Look for processes running out of or accessing files that have been unlinked (i.e., link count is zero). An attacker may be hiding data in or running a backdoor from such files:

```
# lsof +L1
```

On a Linux machine with RPM installed (RedHat, Mandrake, etc.), run the RPM tool to verify packages:

```
# rpm -Va | sort
```

This checks size, MD5 sum, permissions, type, owner, and group of each file with information from the RPM database to look for changes. Output includes:

```
S - File size differs
M - Mode differs (permissions)
5 - MD5 sum differs
D - Device number mismatch
L - readLink path mismatch
U - user ownership differs
G - group ownership differs
T - modification time differs
```

Pay special attention to changes associated with items in /sbin, /bin, /usr/sbin, and /usr/bin.

In some versions of Linux, this analysis is automated by the built-in `check-packages` script.

## Unusual Network Usage

Look for promiscuous mode, which might indicate a sniffer:

```
# ip link | grep PROMISC
```

Note that the `ifconfig` doesn't work reliably for detecting promiscuous mode on Linux kernel 2.4, so please use "ip link" for detecting it.

## Unusual Network Usage Continued

Look for unusual port listeners:

```
# netstat -nap
```

Get more details about running processes listening on ports:

```
# lsof -i
```

These commands require knowledge of which TCP and UDP ports are normally listening on your system. Look for deviations from the norm.

Look for unusual ARP entries, mapping IP address to MAC addresses that aren't correct for the LAN:

```
# arp -a
```

This analysis requires detailed knowledge of which addresses are supposed to be on the LAN. On a small and/or specialized LAN (such as a DMZ), look for unexpected IP addresses.

## Unusual Scheduled Tasks

Look for cron jobs scheduled by root and any other UID 0 accounts:

```
# crontab -u root -l
```

Look for unusual system-wide cron jobs:

```
# cat /etc/crontab
# ls /etc/cron.*
```



# Upcoming SANS Training

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

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced