SANS Institute
Security Consensus Operational Readiness Evaluation
This checklist is from the SCORE Checklist Project. Reposting is not permited 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)
- 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

Tripwire looks for changes to critical system files – 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.

The free Bastille Script provides automated security hardening for Linux systems, available at www.bastille-linux.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 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 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 Munich March 2018	**Munich, DE**	**Mar 19, 2018 - Mar 24, 2018**	**Live Event**
SANS Pen Test Austin 2018	**Austin, TXUS**	**Mar 19, 2018 - Mar 24, 2018**	**Live Event**
SANS Secure Canberra 2018	**Canberra, AU**	**Mar 19, 2018 - Mar 24, 2018**	**Live Event**
SANS Boston Spring 2018	**Boston, MAUS**	**Mar 25, 2018 - Mar 30, 2018**	**Live Event**
SANS 2018	**Orlando, FLUS**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Abu Dhabi 2018	**Abu Dhabi, AE**	**Apr 07, 2018 - Apr 12, 2018**	**Live Event**
Pre-RSA® Conference Training	**San Francisco, CAUS**	**Apr 11, 2018 - Apr 16, 2018**	**Live Event**
SANS Zurich 2018	**Zurich, CH**	**Apr 16, 2018 - Apr 21, 2018**	**Live Event**
SANS London April 2018	**London, GB**	**Apr 16, 2018 - Apr 21, 2018**	**Live Event**
SANS Baltimore Spring 2018	**Baltimore, MDUS**	**Apr 21, 2018 - Apr 28, 2018**	**Live Event**
Blue Team Summit & Training 2018	**Louisville, KYUS**	**Apr 23, 2018 - Apr 30, 2018**	**Live Event**
SANS Seattle Spring 2018	**Seattle, WAUS**	**Apr 23, 2018 - Apr 28, 2018**	**Live Event**
SANS Riyadh April 2018	**Riyadh, SA**	**Apr 28, 2018 - May 03, 2018**	**Live Event**
SANS Doha 2018	**Doha, QA**	**Apr 28, 2018 - May 03, 2018**	**Live Event**
SANS SEC460: Enterprise Threat Beta Two	**Crystal City, VAUS**	**Apr 30, 2018 - May 05, 2018**	**Live Event**
Automotive Cybersecurity Summit & Training 2018	**Chicago, ILUS**	**May 01, 2018 - May 08, 2018**	**Live Event**
SANS SEC504 in Thai 2018	**Bangkok, TH**	**May 07, 2018 - May 12, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CAUS**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS Melbourne 2018	**Melbourne, AU**	**May 14, 2018 - May 26, 2018**	**Live Event**
SANS Northern VA Reston Spring 2018	**Reston, VAUS**	**May 20, 2018 - May 25, 2018**	**Live Event**
SANS Amsterdam May 2018	**Amsterdam, NL**	**May 28, 2018 - Jun 02, 2018**	**Live Event**
SANS Atlanta 2018	**Atlanta, GAUS**	**May 29, 2018 - Jun 03, 2018**	**Live Event**
SANS Rocky Mountain 2018	**Denver, COUS**	**Jun 04, 2018 - Jun 09, 2018**	**Live Event**
SANS London June 2018	**London, GB**	**Jun 04, 2018 - Jun 12, 2018**	**Live Event**
DFIR Summit & Training 2018	**Austin, TXUS**	**Jun 07, 2018 - Jun 14, 2018**	**Live Event**
SANS Milan June 2018	**Milan, IT**	**Jun 11, 2018 - Jun 16, 2018**	**Live Event**
SEC487: Open-Source Intel Beta One	**OnlineVAUS**	**Mar 19, 2018 - Mar 24, 2018**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**