Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

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.

Intrusion Discovery Cheat Sheet v2.0

Linux

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/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 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.*
```

Last Updated: May 27th, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANSFIRE 2016	Washington, DCUS	Jun 11, 2016 - Jun 18, 2016	Live Event
SANS Pen Test Berlin 2016	Berlin, DE	Jun 20, 2016 - Jun 25, 2016	Live Event
SANS Philippines 2016	Manila, PH	Jun 20, 2016 - Jun 25, 2016	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 23, 2016 - Jun 30, 2016	Live Event
SANS Cyber Defence Canberra 2016	Canberra, AU	Jun 27, 2016 - Jul 09, 2016	Live Event
SANS Salt Lake City 2016	Salt Lake City, UTUS	Jun 27, 2016 - Jul 02, 2016	Live Event
MGT433 at SANS London Summer 2016	London, GB	Jul 07, 2016 - Jul 08, 2016	Live Event
SANS London Summer 2016	London, GB	Jul 09, 2016 - Jul 18, 2016	Live Event
SANS Rocky Mountain 2016	Denver, COUS	Jul 11, 2016 - Jul 16, 2016	Live Event
SANS Delhi 2016	Delhi, IN	Jul 18, 2016 - Jul 30, 2016	Live Event
SANS Minneapolis 2016	Minneapolis, MNUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS San Antonio 2016	San Antonio, TXUS	Jul 18, 2016 - Jul 23, 2016	Live Event
Industrial Control Systems Security Training	Houston, TXUS	Jul 25, 2016 - Jul 30, 2016	Live Event
SANS San Jose 2016	San Jose, CAUS	Jul 25, 2016 - Jul 30, 2016	Live Event
SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
Security Awareness Summit & Training	San Francisco, CAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Dallas 2016	Dallas, TXUS	Aug 08, 2016 - Aug 13, 2016	Live Event
SANS Portland 2016	Portland, ORUS	Aug 08, 2016 - Aug 13, 2016	Live Event
Data Breach Summit	Chicago, ILUS	Aug 18, 2016 - Aug 18, 2016	Live Event
SANS Virginia Beach 2016	Virginia Beach, VAUS	Aug 22, 2016 - Sep 02, 2016	Live Event
SANS Chicago 2016	Chicago, ILUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS Bangalore 2016	Bangalore, IN	Aug 22, 2016 - Sep 03, 2016	Live Event
SANS Alaska Summit & Training	Anchorage, AKUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS SEC401 Luxembourg en francais	OnlineLU	May 30, 2016 - Jun 04, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced