Unusual Accounts

Look in /etc/passwd for new accounts, especially with UID 0 or GID 0

```
# less /etc/passwd
# grep :0: /etc/passwd
```

Normal accounts will be there, but look for new, unexpected accounts

Unusual Log Entries

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

Promiscuous mode
"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 (-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)

For web servers: Large number of Apache logs saying "error"

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.

Chkrootkit looks for anomalies on systems introduced by user-mode and kernel-mode RootKits
www.chkrootkit.org - free

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

SANS INSTITUTE

Intrusion Discovery Cheat Sheet *Linux*

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 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 unusual processes, getting more detail using:
lsof –p [pid]

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

Unusual Files

Look for unusual SUID root files:
find / -uid 0 –perm -4000 –print
Requires knowledge of normal SUID files

Look for unusual large files (greater than 10 MegaBytes):
find / -size +10000k –print

Requires knowledge of normal large files

Look for files named with dots and spaces:
(“…”, “.. “, “. “, and “ “)
find / -name “...“ –print
find / -name “.. “ –print
find / -name “. “ –print
find / -name “ “ –print

Unusual Files Continued

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

rpm –Va

Checks size, MD5 sum, permissions, type, owner, and group of each file with information from RPM database

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

Unusual Network Usage

Look for promiscuous mode, which might indicate a sniffer:

ip link | grep PROMISC

Note that ifconfig doesn’t work reliably for detecting promiscuous mode on Linux kernel 2.4

Unusual Network Usage Continued

Look for unusual port listeners:
lsof –i
netstat –nap

Need to know which TCP and UDP ports are normally listening on your system and 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

Requires detailed knowledge of what is supposed to be on the LAN

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.*