Idea: run something regularly (at least on managed machines) and perhaps on desktops that looks for signs of a compromise. See also LinuxHardening and RootKitCheckerInternal.

Criteria:

- zero false positive (FP) rate (or as close as possible). This tool will generate additional work...
- no CERN-only tool - we need to benefit from upstream updates to "signatures" with minimal delay
- integration with automatic updates, no separately maintained checksums if possible
- run as cron job, run on demand

Docs:

- Samhain article on how kernel-level rootkits
- chkrootkit's link collection to various rootkits
- SuckIt kernel-level rootkit - on-the-fly patching via /dev/kmem (no modules)
- Abuse of the Linux Kernel for Fun and Profit, by halflife, Phrack 50, April 9, 1997 - classic seminal paper
- The Hacker's Choice on loadable kernel modules - various papers on how to subvert Linux kernels
- Gabe_Lawrence at Toorcon 2007 nice timelline for the various rootkit generations

For testing the efficiency of the detection, we should probably have a collection of rootkits (brrr..). Fortunately, from time to time generous people supply these...

cern-rpmverify

CERN-tool, written by A.Earl, runs e.g. on LXPLUS. Configured via ncm-rpmverify. RPM-md5 checksummer with some known FP elimination. More documentation here

chkrootkit

http://chkrootkit.org

- file location signatures
- some kernel-level detections (`ps` vs `/proc` view, syscall-table hooking). will **not** detect Interrupt Descriptor Table (IDT) replacements
- Lionel rewrote this in perl some time ago (with less FPs), but not updated since (froze SLC4?). Available from `/afs/cern.ch/project/security/cern/public/tools/check-rootkit/`

rkhunter (Use for CERN)

http://sf.net/projects/rkhunter , Lead developer's blog

- currently undergoing rewrite, revived after some dormancy - 1.3.2 is out.
- file location signatures (not in /tmp ?), strings, "bad" checksums, "known good" checksums for some binaries
- several patches submitted, some accepted.
- RPMified, cron-ified.
- shell script: heavy/slow (10k processes per run)

Questions:

- what about /tmp, /var/tmp etc ? no checks yet.. `suspscan` has lots of false positives.

- can we leverage slocate/updatedb runs instead of crawling ourselves? at least for "weird" names?
- what about Viruses (e.g. "grep" infected, heavily used?) - detected via RPM checksum
- kernel-level RK detection is weak - blacklist of module names only, no "=ps= vs /proc" checks (update - now included `unhide` binary)
- now uses RPM-md5.
- unclear future after ownership change - not all directions look useful to us:
  - "this application version is old and vulnerable"-counseling, but not up-to-date - can disable
  - internationalization - lots of complexity
  - lots of effort into beautification (coloured output)

Good candidate for now, but only with a suitable CERNified configuration. Available on SLC4, SLC5,includes checking cronjob,

Samhain

http://www.la-samhna.de/samhain/s_faq.html

- centralized do-it-all system - from centralized logging to application deployment. Hard to integrate with existing tools
- originally a checksum-based system, now has some add-on modules (kernel check - does not work on SLC4, open ports, new SUID programs)

zeppoo (DEAD project)

kernel-level rootkit detection - only. Interesting ideas. was at ~~http://www.zeppoo.net~~ (now gone/replaced by redirector).

- requires full read access to /dev/mem
  - not available on SLC4 (where /dev/kmem is gone, and /dev/mem only allows access to "low" PCI memory etc).
  - Their solution: "disable the lowpage protection" by binary patching the kernel via /dev/mem :((so much for this being a good protection, any rootkit can do the same)
  - recipe at http://www.zeppoo.net/articles/UseRedhat, and this can be scripted...
- RPMified (by Jan), but couldn't get it to really work.

rootcheck

http://www.ossec.net/en/rootcheck.html

- RPMified by Jan

the99lb

toorcon 2007 talk at http://toorcon.org/2007/talks/11/Gabe_Lawrence.ppt

Is more focused on live analysis/dump, i.e. load some module post-incident, dump changed structures, some userspace debugging/rev engineering to find out what happened to the box.

code available from `svn co https://the99lb.svn.sourceforge.net/svnroot/the99lb the99lb` (rest of SF page is pretty empty)

Includes kernel module to dump IDT, syscall table, does not compile on Xen...

Rootkit Profiler LX (RKProfiler) (DEAD project)

http://www.trapkit.de/research/rkprofiler/

(from the announcement BugTraq 19.02.2007):

KProfiler LX is divided into two parts: a data collection component called "Rootkit Profiler Module" (RKPmod) and a data interpretation component called "Rootkit Profiler Console" (RKPconsole).

RKPmod is a kernel module that gets loaded on the system that should be checked for the presence of a kernel rootkit. There are other ways to perform data collection, but currently only this approach is publicly available.

RKPconsole is a userland program that can be used to analyse the collected information.

RKProfiler LX checks the whole kernel code as well as different kernel data sections and cpu registers regarding possible modifications and hidden components:

- Generic kernel code modification
- Syscall table address modification
- Syscall address modification
- Syscall code modification
- Interrupt handler address modification
- Interrupt handler code modification
- Page Fault Handler modification
- Kernel symbol modification
- SYSENTER register modification
- Virtual File System function pointer modification
- Hidden processes and threads
- Hidden kernel modules

Will not test right now - freeware but not open source, with binary-modules only for SuSE and Ubuntu stock kernels. Appears to use whitelist hashes for kernel code, and pointer validations.

January 2008: author might be willing to opensource this. September 2008: still no updates/license changes, marked as `!!! THE PROJECT IS NOT FURTHER MAINTAINED AT THE MOMENT !!!`

commercial product: Symantec Antivirus for Linux

(we already use SAV for Window)

Documentation: SAV_Linux_Impl.pdf linux_readme.txt SAV_Linux_Client.pdf

- Classical signature-based antivirus
- optional kernel module (binary-only, only available for selected vendor kernels - i.e. not SLC4) will block "bad" programs

Need to sort out license - per-machine, site-license, redistributable?

This topic: LinuxSupport > RootKitChecker
Topic revision: r10 - 2009-01-22 - JanIven