chkrootkit -- locally checks for signs of a rootkit

By Nelson Murilo, Klaus Steding-Jessen

Archived: 2026-04-06 00:21:09 UTC

chkrootkit is a tool to locally check for signs of a rootkit. It contains:

- **chkrootkit**: shell script that checks system binaries for rootkit modification.
- **ifpromisc.c**: checks if the interface is in promiscuous mode.
- **chklastlog.c**: checks for lastlog deletions.
- **chkwtmp.c**: checks for wtmp deletions.
- **check_wtmpx.c**: checks for wtmpx deletions. (Solaris only)
- **chkproc.c**: checks for signs of LKM trojans.
- **chkdirs.c**: checks for signs of LKM trojans.
- **strings.c**: quick and dirty strings replacement.
- **chkutmp.c**: checks for utmp deletions.

Chkrootkit is named Top 10 Tools to Scan Linux Servers for Vulnerability and Malware by Cyber Security News.
After 25 years still helping people around world!

What's New

chkrootkit 0.59 is now available! (Release Date: Jan 01 2026)

This version includes:

- chkrootkit
  - New checks: Process executed from memory
  - New commands: nologin
  - XZ Backdoor Bottkitty (UEFI Bootkit)
  - Bug fixes

Tests performed and rootkits detected

The following tests are made:

- `aliens asp bindshell lkm rexedcs sniffer w55808 wted scalper slapper z2 chkutmp OSX_RSPLUG amd basename biff chfn chsh cron crontab date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf identd init killall ldsopreload login ls lsof mail mingetty netstat named passwd`

```
pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail
sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w
write
```

The following rootkits, worms and LKMs are currently detected:

01. lrk3, lrk4, lrk5, lrk6 (and variants);	02. Solaris rootkit;	03. FreeBSD rootkit;
04. t0rn (and variants);	05. Ambient's Rootkit (ARK);	06. Ramen Worm;
07. rh[67]-shaper;	08. RSHA;	09. Romanian rootkit;
10. RK17;	11. Lion Worm;	12. Adore Worm;
13. LPD Worm;	14. kenny-rk;	15. Adore LKM;
16. ShitC Worm;	17. Omega Worm;	18. Wormkit Worm;
19. Maniac-RK;	20. dsc-rootkit;	21. Ducoci rootkit;
22. x.c Worm;	23. RST.b trojan;	24. duarawkz;
25. knark LKM;	26. Monkit;	27. Hidrootkit;
28. Bobkit;	29. Pizdakit;	30. t0rn v8.0;
31. Showtee;	32. Optickit;	33. T.R.K;
34. MithRa's Rootkit;	35. George;	36. SucKIT;
37. Scalper;	38. Slapper A, B, C and D;	39. OpenBSD rk v1;
40. Illogic rootkit;	41. SK rootkit.	42. sebek LKM;
43. Romanian rootkit;	44. LOC rootkit;	45. shv4 rootkit;
46. Aquatica rootkit;	47. ZK rootkit;	48. 55808.A Worm;
49. TC2 Worm;	50. Volc rootkit;	51. Gold2 rootkit;
52. Anonoying rootkit;	53. Shkit rootkit;	54. AjaKit rootkit;
55. zaRwT rootkit;	56. Madalin rootkit;	57. Fu rootkit;
58. Kenga3 rootkit;	59. ESRK rootkit;	60. rootedoor rootkit;
61. Enye LKM;	62. Lupper.Worm;	63. shv5;

64. OSX.RSPlug.A;	65. Linux Rootkit 64Bit;	66. Operation Windigo;
67. Mumblehard backdoor/botnet;	68. Linux.Xor.DDoS Malware;	69. Backdoors.linux.Mokes.a;
70. Linux.Proxy.10	71. Rocke Monero Miner	72. Umbreon Linux Rootkit
73. Linux BPFDoor	74. Kovid Rootkit	75. Syslogk Rootkit

chkrootkit has been tested on: Linux 2.0.x, 2.2.x, 2.4.x and 2.6.x, 3x, 4x and 5x. FreeBSD 2.2.x, 3.x, 4.x, 5.x, 7.x and 10.x, OpenBSD 2.x, 3.x, 4.x and 5.x., NetBSD 1.6.x, Solaris 2.5.1, 2.6, 8.0 and 9.0, HP-UX 11, Tru64, BSDI and Mac OS X.

More details can be found on the chkrootkit's README.

Support us:

Chkrootkit is free software. However, large amounts of time and effort go into its continued development. If you are interested in financially supporting the development of Chkrootkit, please send your donation to nelsonmurilo[at]gmail.com via PayPal.
We accept Bitcoin as well
If you like our work, please consider supporting Chkrootkit at Patreon. Thank you.
Chkrootkit shop (NEW): Shop here!

Contacting the Authors: Please send comments, new rootkits, questions and bug reports to Nelson Murilo <nmuriloat.gmail.com> (main author) and Klaus Steding-Jessen <jessen@cert.br> (co-author).

Discover more

linux

Linux & Unix

Computer Security

Source: http://www.chkrootkit.org/