Rootkits

Pat TenHoopen - WMLUG

What is a rootkit?

A rootkit is a program that, once installed, tries to hide itself from detection.

It does not grant administrative-user privileges. It has to be installed by someone with the rights to modify the file system.

What is a Rootkit?

The purpose or function of the rootkit will vary depending on what it was written to do.

Some rootkits install keyloggers, provide back-doors for access, but in general, they provide access to the system to unauthorized users.

Rootkits vs Viruses

A rootkit will not normally try to spread to other systems once it is installed, unlike a virus, but it will try to maintain its control of the system.

A rootkit may be installed by a virus, usually in the form of a trojan.

How Do Rootkits Get Installed?

Rootkits need to be installed by a administrative-level user.

This can be accomplished by physical access to the system, or by the unwitting installation of applications or device drivers that contain a trojan, by the system admin.

Checking For Rootkits

Checking for rootkit installers can be accomplished before the system is compromised through signature scanning of files by an anti-virus program.

However, once the rootkit has been executed, the system cannot be trusted, as the rootkit goes into stealth mode and modifies the scanning results to hide itself.

Checking For Rootkits

For example, the rootkit will most likely modify the output of a process list so that it doesn't show itself.

Likewise, a file listing will not show the rootkit's files.

Checking For Rootkits

The most effective way to check for a rootkit is to boot the system from a trusted, clean OS source (live CD) and scan the system.

The rootkit isn't active at that point and can be detected either through its own files being found or utilities and drivers being compared to clean copies. If they differ, then they are most likely compromised.

Detector - chkrootkit

chkrootkit
http://www.chkrootkit.org/

chkrootkit is a tool that checks for signs of a rootkit.

It checks for changes in binaries, NIC promiscuous mode, lastlog deletion, log tampering, rootkit config files, and hidden processes.

chkrootkit has been tested on:

Linux 2.0.x, 2.2.x, 2.4.x and 2.6.x, FreeBSD 2.2.x, 3.x, 4.x and 5.x, OpenBSD 2.x, 3.x and 4.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

Chkrootkit detection list

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;

Detector - rkhunter

Rootkit Hunter

http://www.rootkit.nl/projects/rootkit_hunter.html

Rootkit Hunter (rkhunter) is a rootkit scanning tool.

It checks for changes in binaries, rootkit files, hidden files, and wrong binary permissions, among other things.

It is supported on most Linux and BSD distributions, and Solaris SunOS. It is not supported on NetBSD.

rkhunter detection list

The following rootkits/backdoors/LKM's/worms are detected:

55808 Trojan - Variant A, ADM W0rm, AjaKit, aPa Kit, Apache Worm, Ambient (ark) Rootkit, Balaur Rootkit, BeastKit, beX2, BOBKit, CiNIK Worm (Slapper.B variant), Danny-Boy's Abuse Kit, Devil RootKit, Dica, Dreams Rootkit, Duarawkz Rootkit, Flea Linux Rootkit, FreeBSD Rootkit, Fuck`it Rootkit, GasKit, Heroin LKM, HjC Rootkit, ignoKit, ImperalsS-FBRK, Irix Rootkit, Kitko, Knark, Li0n Worm, Lockit / LJK2, mod_rootme (Apache backdoor), MRK, Ni0 Rootkit, NSDAP (RootKit for SunOS), Optic Kit (Tux), Oz Rootkit, Portacelo, R3dstorm Toolkit, RH-Sharpe's rootkit, RSHA's rootkit, Scalper Worm, Shutdown, SHV4 Rootkit, SHV5 Rootkit, Sin Rootkit, Slapper, Sneakin Rootkit, Suckit, SunOS Rootkit, Superkit, TBD (Telnet BackDoor), TeLeKiT, T0rn Rootkit, Trojanit Kit, URK (Universal RootKit), VcKit, Volc Rootkit, X-Org SunOS Rootkit, zaRwT.KiT Rootkit

Others:

Anti Anti-sniffer
LuCe LKM
THC Backdoor

Detector - OSSEC

OSSEC
http://www.ossec.net/main/

OSSEC is an Open Source Host-based Intrusion Detection System (HIDS).

It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

It runs on most operating systems, including Linux, Mac OS, Solaris, HP-UX, AIX and Windows.

Other Tools

These tools are meant to be run before infection, and periodically thereafter to check for system changes:

AIDE (Advanced Intrusion Detection Environment)
http://www.cs.tut.fi/~rammer/aide.html

AIDE is a free replacement for Tripwire. It does the same things as the semi-free Tripwire and more.

AFICK (Another File Integrity Checker)
http://afick.sourceforge.net/

AFICK is a security tool, very close from the well known Tripwire. It allows to monitor the changes on your files systems, and so can detect intrusions.

Removal

What do you do if a checker finds a rootkit or you suspect you have one?

Removal

What do you do if a checker finds a rootkit or you suspect you have one?

Easy way: Reformat and reinstall the OS

Removal

What do you do if a checker finds a rootkit or you suspect you have one?

Easy way: Reformat and reinstall the OS

Hard way: Boot with a clean, read-only copy of an OS (via live CD, etc.) and remove the infected files manually

More Info on Rootkits

For more information, see:

http://linuxhelp.blogspot.com/2006/12/various-ways-of-detecting-rootkits-in.html

http://en.wikipedia.org/wiki/Rootkit

Conclusion

A binary's download source/repository should be verified as legitimate and the files checked with an anti-virus/rootkit scanner before installation.

Physical security of a system is also vital.

Although rootkits may not be extremely prevalent, using a rootkit checker along with file integrity checker should be considered good practice.

Questions?

?

Thank You

Thank you for your time and attention!