Table Of Contents

Table Of Contents 1
Detecting rootkits under Linux 2
Zeppoo Software 2
Chkrootkit Software 2
rkhunter software 2
Recommended readings: man pages - rkhunter and chkrootkit rkhunter [4] Project home page chkrc 3

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Linux Detecting / Checking Rootkits with Chkrootkit and rkhunter Software

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. Most rootkits use the power of the kernel to hide themselves, they are only visible from within the kernel. How do I detect rootkits under CentOS or Debian Linux server?

A.. A rootkit is a program [2] (or combination of several programs) designed to take fundamental control (in Unix terms "root" access, in Windows terms "Administrator" access) of a computer system, without authorization by the system's owners and legitimate managers.

Detecting rootkits under Linux

You can try the following tools to detect Linux rootkits:

WARNING! These examples should run from Live CD (Linux Live Security CD) for the best result.

Zeppoo Software

Zeppoo - Zeppoo allows you to detect rootkits on i386 and x86_64 architecture under Linux, by using /dev/kmem and /dev/mem. Moreover it can also detect hidden tasks, connections, corrupted symbols, system calls and so many other things. Download source code here [3]

Chkrootkit Software

Chkrootkit - chkrootkit is a tool to locally check for signs of a rootkit. Type the following command to install chkrootkit

```
$ sudo apt-get install chkrootkit
```

Start looking for rootkits, enter:

```
$ sudo chkrootkit
```

Look for suspicious strings, enter:

```
$ sudo chkrootkit -x | less
```

You need to specify the path for the external commands used by chkrootkit such as awk, grep and others. Mount /mnt/safe using nfs in read-only mode and set /mnt/safe binaries PATH as trusted one, enter:

```
$ sudo chkrootkit -p /mnt/safe
```

rkhunter software

rkhunter - rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors and possible local exploits. rkhunter is a shell script which carries out various checks on the local system to try and detect known rootkits and malware. It also performs checks to see if commands have been modified, if the system startup files have been modified, and various checks on the network interfaces, including checks for listening applications. Type the following command to install rkhunter:

```
$ sudo apt-get install rkhunter
```

The following command option tells rkhunter to perform various checks on the local system:

```
$ sudo rkhunter --check
```

The following command option causes rkhunter to check if there is a later version of any of its text data files:

```
$ sudo rkhunter --update
```

The following option tells rkhunter which directories to look in to find the various commands it requires:

```
$ sudo rkhunter --check --bindir /mnt/safe
```

Recommended readings:

- **man pages - rkhunter and chkrootkit**
- **rkhunter [4] Project home page**
- **chkrootkit [5] Project home page**

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/howto-check-linux-rootkist-with-detectors-software/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/linux/**
[2] A rootkit is a program: **http://en.wikipedia.org/wiki/Rootkit**
[3] here: **http://sourceforge.net/projects/zeppoo**
[4] rkhunter: **http://rkhunter.sourceforge.net/**
[5] chkrootkit: **http://www.chkrootkit.org/**

Copyright © 2006-2010 nixCraft. All rights reserved. This print / pdf version is for personal non-commercial use only. More details http://www.cyberciti.biz/tips/copyright.