

chkrootkit howto

1. Vorwort
2. Chkrootkit besorgen
3. Installation
4. Auf root kit's testen
5. Auswertung
6. Irrtümer

1. Vorwort:

Ich beschreibe in diesem Howto, wie man seine *nix Maschine auf Rootkits überprüft, leider erkennt Chkrootkit nicht alle Root Kit's. Solltet ihr immernoch der Annahme sein "meine Kiste wird schon nicht gehackt werden", so liegt ihr definitiv falsch. Auch ich habe mal so gedacht, das Ende vom Lied war, dass mein Red Hat 9 Server, welcher eine von T-online zugewiesene IP-Adresse hat, gerootet wurde, aufgefallen ist mir das nur dadurch, dass von heute auf morgen ein neuer Port offen war. Also fühlt euch nicht sicher, sondern überprüft eure Systeme lieber auf Root Kit's. Chkrootkit ist dazu ein guter Anfang.

2. Chkrootkit besorgen:

Wir laden uns die neueste Version von Chkrootkit von www.chkrootkit.org herunter, dabei sollte es sich um ein gepacktes Archiv (tar.gz) handeln. Wichtig: Nach dem Download müssen alle weiteren Vorgänge als root (uid 0) ausgeführt werden.

3. Installation

Wir entpacken das herunter geladene Archiv per "tar -xvzf <filename>". <filename> müsst ihr natürlich durch den richtigen Dateinamen ersetzen. Danach wechseln wir per "cd chkrootkit*" in das Verzeichnis in welches wir unser Archiv entpackt haben. Da wir hier nur die Quellen haben, müssen wir die ganze Geschichte nun noch compilieren, das geschieht mit make. Damit wäre die Installation auch schon abgeschlossen.

4. Testen auf Root Kit's:

Getestet wird das System ganz einfach der ./chkrootkit. Dies muss als Root geschehen, da das Tool sonst keinen Zugriff auf /dev/kmem oder andere Devices bekommt, was zum Testen jedoch nötig ist.

5. Auswertung:

Sollte irgendwo etwas von infected oder ähnlichem beim Test stehen, so könnt ihr ziemlich sicher sein ein Rootkit auf der Kiste zu haben. Auch der Promiscmode auf Netzwerk-devices ist ein Indiz für einen Einbruch, natürlich nur dann, wenn ihr die Karte/Verbindung nicht selber in den Promiscmode versetzt habt.

6. Irrtümer:

Es kann durchaus vorkommen, dass chkrootkit irrtümlich Root Kit's meldet, das kann unter anderem dadurch passieren, dass ihr Programme

verändert habt und diese dann denen eines Root Kits sehr ähnlich sind. Also verlasst euch nicht blind auf die Software, aber ignoriert die Warnungen auch nicht, sondern überprüft euer System lieber nochmal auf leere Logfiles etc.