|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| chkrootkit  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  chkrootkit (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png |  | Identification des rootkits  chkrootkit est un logiciel libre sous licence GNU GPL permettant de détecter si un système Linux n'a pas été compromis par un rootkit.  Il permet de détecter les traces d'une attaque et de rechercher la présence d'un *rootkit* sur un système en vérifiant les points suivants :   * si des fichiers exécutables du système ont été modifiés ; * si l’interface réseau est en mode « *promiscuous* » ; * si un ou des vers LKM (*Loadable Kernel Module*) sont présents.   La vérification effectuée au sujet du mode *promiscuous* consiste à voir si l’interface réseau est configurée pour récupérer et lire toutes les trames, indiquant ainsi la possibilité qu'un sniffer soit installé sur le système.  La définition exacte de rootkit donnée par Wikipedia est …  « ensemble d'exploits réunis afin d'avoir des chances maximales de voler un compte *root* (administrateur), c'est-à-dire avec lequel on peut faire n'importe quoi. sur une machine Linux. »  Les binaires suivants sont vérifiés …   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **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** |  |   … ainsi que toute une série de vérifications (vers, *sniffer's*, LKM...)  **Installation**  **>> sudo** **apt update**  **>> sudo** **apt --yes upgrade**  **>> sudo** **apt --yes install chkrootkit**  **Utilisation**  **>> sudo chkrootkit**  ou  **>> sudo chkrootkit > resultat.chkrootkit**  Le plus difficile pour vous sera de déterminer les "faux positifs"...  En effet, il arrivera que chkrootkit produise des alertes qui ne sont pas justifiées.  **Références**  <https://www.isalo.org/wiki.debian-fr/Chkrootkit>  **Site officiel**  <http://www.chkrootkit.org/> |
|  |  |  |