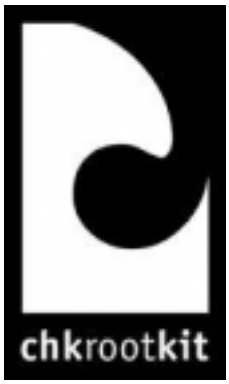
Chkrootkit - поиск в системе rootkit и backdoor

Опубликовано muff в Ср, 2012-12-05 14:37



Попросили "посмотреть" сервер, который несколько лет работал в штатном режиме без стороннего вмешательства. Свои задачи он исправно исполнял, планировалось расширение функционала... Под "шумок" решил провести тестирование системы на наличие уязвимостей и присутствия "заразы". Как никак - несколько лет работы без обновлений софта...

Данные о тестируемой системе:

```
# uname -v
 FreeBSD 7.0-RELEASE-p3 #0: Mon Aug  4 13:49:40 EEST 2008     root [at] arey [dot]
local:/usr/obj/usr/src/sys/AREY
```

Для проверки на наличие руткитов и бекдоров, воспользуемся утилитой **chkrootkit**. Это сканер системы безопасности, который ищет в системе признаки, указывающие на наличии в системе руткитов (*англ. **rootkit**, т.е. "набор root'а" - программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе*) или бекдоров (*от англ. **back door**, чёрный ход - программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе*).

Однако, имейте ввиду, что проверка только данным сканером не дает гарантии, что система не подвергалась взлому. Вместе с **chkrootkit** используйте также дополнительный софт.

Выполним установку **chkrootkit** из системы портов, которые предварительно необходимо обновить [1]:

```
# cd /usr/ports/security/chkrootkit && make install clean && rehash
```

После установки для использования утилиты доступны следующие ключи:

```
Usage: /usr/local/sbin/chkrootkit [options] [test ...]Options:        -h
    ?????????? ??? ????????? ? ?????        -V               ?????????? ??????????
? ?????? ? ?????        -l               ?????????? ?????? ????????? ?????? ? ?????
        -d                ???????        -q               "?????" ?????        -x
             ?????????? ?????        -r dir            ??????????? ??????? ???????
 ??? ???????? ??????????        -p dir1:dir2:dirN ???? ? ??????? ??????????, ???????
 ?????????? chkrootkit        -n               ?????????? ?????????????????? ????????
 NFS
```

В ходе работы **chkrootkit** отправляет следующие уведомления:

- **INFECTED** - даная программа может относиться к известным образцам враждебного

кода (rootkit)
- **not infected** - отсутствие сигнатур известных руткитов
- **not tested** - тест не выполнен по одной из указанных причин
    - неприменимость проверки для даной ОС
    - отсутствие возможности использования внешней программы
    - заданы опции коммандной строки, отключающие эту проверку
- **not found** - программа не найдена, поэтому не проверялась
- **Vulnerable but disabled** - программа заражена, но на момент проверки не используется (не запущена)

Проверим, какая версия **chkrootkit** была установлена:

```
# chkrootkit -V

chkrootkit version 0.49
```

Что ж... Кажется пора выполнить проверку. Для этого запустим утилиту, без использования ключей:

```
# chkrootkit

ROOTDIR is `/'
Checking `amd'... not infected
Checking `basename'... not infected
Checking `biff'... not infected
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not infected
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not found
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not infected
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not tested
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not found
Checking `mail'... not infected
Checking `mingetty'... not found
Checking `netstat'... not infected
Checking `named'... not infected
Checking `passwd'... not infected
Checking `pidof'... not found
Checking `pop2'... not found
Checking `pop3'... not found
```

```
Checking `ps'... not infected
Checking `pstree'... not found
Checking `rpcinfo'... not infected
Checking `rlogind'... not infected
Checking `rshd'... not infected
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not infected
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not infected
Checking `timed'... not infected
Checking `traceroute'... not infected
Checking `vdir'... not found
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... nothing found
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for OBSD rk v1... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found
```

```
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... INFECTED (PORTS:  465)
 Checking `lkm'... chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... fxp0 is not promisc
vlan1 is not promisc
vlan2 is not promisc
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'... chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not infected
```

Согласно отчета, система инфицирована. Необходимо разобраться что да как... Chkrootkit "ругается" на открытый порт 465 (smtp protocol over TLS/SSL). Однако на даном сервере работает почтовый сервер, который и настроен на работу по **smtps**. Если в настройках почтового сервера отключить работу по **smtps**, то проверка проходит корректно, соответственно можно данный случай считать ложным срабатыванием.

Источник (получено *2024-09-21 05:33*):
http://muff.kiev.ua/content/chkrootkit-poisk-v-sisteme-rootkit-i-backdoor

Ссылки:
[1] http://muff.kiev.ua/content/csup-obnovlyaem-sistemu