Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Николай Малых

Использование программы chkrootkit для мониторинга

http://www.chkrootkit.org

Программа **chkrootkit** предназначена для поиска враждебного кода (rootkit) и иных подозрительных событий в системе. Программа включает в себя несколько модулей:

- **chkrootkit** – сценарий проверки системы;
- **ifpromisc** – поиск интерфейсов, работающих в режиме захвата пакетов.
- **chklastlog** – обнаружение фактов удаления записей из журнального файла **lastlog**.
- **chkwtmp** – обнаружение фактов удаления записей из журнального файла **wtmp**.
- **check_wtmpx** – обнаружение фактов удаления записей из журнального файла (только для ОС Solaris).
- **chkproc** – поиск следов троянских программ LKM[1].
- **chkdirs** – поиск следов троянских программ LKM.
- **strings** – программа для быстрого поиска и замены текстовых строк.

Модули **chkwtmp** и **chklastlog** пытаются обнаруживать факты удаления записей из системных журналов **wtmp** и **lastlog**, но полное обнаружение всех изменений этих файлов не гарантируется.

Предпринимаются попытки поиска файлов, собранных анализаторами (тест aliens) в обычных местах расположения подобных файлов. Возможность нестандартного расположения файлов не позволяет гарантировать их обнаружение во всех случаях.

Модуль **chkproc** проверяет файлы **/proc** для обнаружения скрытых от команд **ps** и **readdir** системных вызовов, которые могут быть связаны с троянскими модулями LKM. Вы можете использовать эту команду с ключом **-v** для вывода более подробного отчета.

Chkrootkit может обнаруживать широкий спектр враждебного кода, перечисленного ниже.

lrk3, lrk4, lrk5, lrk6 (и варианты)	dsc-rootkit	OpenBSD rk v1
Solaris rootkit	Ducoci rootkit	Illogic rootkit
FreeBSD rootkit	x.c Worm	SK rootkit
t0rn (и варианты)	RST.b trojan	sebek LKM
Ambient's Rootkit (ARK)	duarawkz	Romanian rootkit
Ramen Worm	knark LKM	LOC rootkit
rh[67]-shaper	Monkit	shv4 rootkit
RSHA	Hidrootkit	Aquatica rootkit
Romanian rootkit	Bobkit	ZK rootkit
RK17	Pizdakit	55808.A Worm
Lion Worm	t0rn v8.0	TC2 Worm
Adore Worm	Showtee	Volc rootkit
LPD Worm	Optickit	Gold2 rootkit
kenny-rk	T.R.K	Anonoying rootkit
Adore LKM	MithRa's Rootkit	Shkit rootkit
ShitC Worm	George	AjaKit rootkit
Omega Worm	SucKIT	zaRwT rootkit
Wormkit Worm	Scalper	Madalin rootkit
Maniac-RK	Slapper A, B, C и D	

Программа работает на различных программных платформах и была успешно протестирована на системах

- Linux с ядрами серий 2.0, 2.2, 2.4 и 2.6;
- FreeBSD 2.2.x, 3.x, 4.x и 5.x;
- OpenBSD 2.x и 3.x.;
- NetBSD 1.5.2;
- Solaris 2.5.1, 2.6 и 8.0;
- HP-UX 11;
- Tru64;
- BSDI.

Для использования программы **chkrootkit** требуются полномочия пользователя root. Простейший способ проверки обеспечивается командой[2]

```
./chkrootkit
```

[1] Loadable Kernel Module – загружаемый модуль ядра.

В этом случае программа будет автоматически выполнять весь набор поддерживаемых тестов. Для выбора отдельных тестов вы можете воспользоваться параметрами командной строки:

```
./chkrootkit [опции] [<имя теста> ...]
```

Опции

Таблица 1 Опции chkrootkit

Опция	*Описание*
-h	Выводит справочную информацию о работе с программой.
-V	Выводит сведения о номере версии программы и завершает работу.
-l	Показывает список поддерживаемых программой проверок.
-d	Задает вывод подробной информации о работе программы (режим отладки).
-q	Задает минимальный вывод информации.
-x	Задает вывод дополнительной информации.
-r <каталог>	Задает имя каталога для использования в качестве корневого (root). Указанный в команде каталог служит стартовой точкой для просмотра дерева каталогов.
-p dir1:dir2:dirN	Указывает пути к внешним программам, используемым **chkrootkit.**
-n	Отключает просмотр смонтированных каталогов NFS.

По умолчанию программа пытается выполнить все доступные проверки, а параметр **<имя теста>** может содержать одно или несколько имен поддерживаемых программой тестов:

aliens	slapper	du	hdparm	login	pop2	sshd	vdir
asp	z2	dirname	su	ls	pop3	syslogd	w
bindshell	amd	echo	ifconfig	lsof	ps	tar	write
lkm	basename	egrep	inetd	mail	pstree	tcpd	
rexedcs	biff	env	inetdconf	mingetty	rpcinfo	tcpdump	
sniffer	chfn	find	identd	netstat	rlogind	top	
wted	chsh	fingerd	init	named	rshd	telnetd	
w55808	cron	gpm	killall	passwd	slogin	timed	
scalper	date	grep	ldsopreload	pidof	sendmail	traceroute	

Например, приведенная ниже команда обеспечивает поиск троянских программ **ps** и **ls**, а также обнаружение интерфейсов, работающих в режиме захвата пакетов.

```
./chkrootkit ps ls sniffer
```

С помощью опции **-q** можно задать работу программы с выводом минимальной информации. В этом случае отчет будет содержать лишь сведения о найденных в системе троянских программах или следах работы анализаторов протоколов и сканеров.

Опция **-x** позволяет пользователю провести поиск подозрительных строк в бинарных файлах, которые могут говорить о присутствии в системе троянских программ. Все решения об идентификации троянских программ пользователь должен будет принять сам. Поскольку в режиме поиска текстовых строк на экран будет выводиться значительный объем информации, целесообразно воспользоваться постраничным выводом:

```
./chkrootkit -x | more
```

Команда

```
./chkrootkit -x | egrep '^/bin'
```

позволяет найти в бинарных файлах текстовые строки, начинающиеся с символов **/bin**, которые могут содержать имена исполняемых файлов. Программа **chkrootkit** может использовать для выполнения проверки другие программы, включая **awk**, **cut**, **egrep**, **find**, **head**, **id**, **ls**, **netstat**, **ps**, **strings**, **sed**, **uname**. Если эти программы недоступны в пути поиска, укажите путь к ним с помощью опции **-p**. Такая возможность позволяет использовать при проверке системы заведомо нормальные версии перечисленных программ, которые могут храниться на отдельном диске без возможности записи на него. Приведенная ниже команда обеспечивает выполнение тестов **chkrootkit** с использованием программ, хранящихся в каталоге **/bin** на компакт-диске, смонтированном в системе как **/cdrom**

```
./chkrootkit -p /cdrom/bin
```

Вы можете указать в командной строке несколько каталогов для поиска требуемых для работы программ, разделяя имена каталогов двоеточием (:)

```
./chkrootkit -p /cdrom/bin:/floppy/mybin
```

Иногда может возникнуть необходимость проверки диска вашей системы на другом компьютере, где заведомо нет враждебного кода. Для этого служит опция **-r** , позволяющая задать точку монтирования для корневого раздела проверяемого диска. Например, при монтировании корневого раздела как **/mnt1**, можно использовать команду:

```
./chkrootkit -r /mnt1
```

[2]Команда должна выполняться из каталога, в котором хранятся исполняемые файлы chkrootkit, поскольку сценарий ищет исполняемые файлы в текущем каталоге, не используя переменную окружения PATH.

Сообщения программы

Ниже перечислены префиксы, используемые программой **chkrootkit** (за исключением случаев использования с опциями **-x** или **-q**) при выводе отчета о проверке:

- **INFECTED** - проверка показала, что данная программа может относиться к известным образцам враждебного кода (rootkit);
- **not infected** – проверка показала отсутствие сигнатур известных rootkit;
- **not tested** – тест не был выполнен по одной из перечисленных ниже причин:
  a) неприменимость проверки для данной ОС;
  b) отсутствие возможности использования требуемой для теста внешней программы;
  c) заданы опции командной строки, отключающие эту проверку (например, **-r**).
- **not found** – программа не была найдена и по этой причине не проверялась;
- **Vulnerable but disabled** – программа заражена, но не используется (не работала в момент проверки или “закомментирована” в **inetd.conf**).

Примеры использования chkrootkit для мониторинга

Программа chkrootkit выводит результаты проверки на консоль, а с помощью стандартных операций вывод может быть направлен в файл.

С помощью chkrootkit можно организовать эффективный мониторинг своей станции и удаленных хостов с передачей результатов проверки по электронной почте. Вы можете включить нужные команды в файл заданий cron для автоматической проверки с желаемой периодичностью. Например, строка

```
0 2 * * * cd /usr/local/bin; ./chkrootkit 2>&1 | mail -s "chkrootkit output for HostName"
root
```

в файле /var/spool/cron/root обеспечит выполнение полного набора тестов в 2 часа 00 минут ежесуточно с передачей отчета локальному пользователю root по электронной почте.

Тест LKM позволяет увидеть в системе процессы, скрытые от утилиты ps, - наличие таких процессов в некоторых случаях может говорить о непорядке в системе, поэтому можно запускать соответствующую команду достаточно часто, чтобы увидеть незваных гостей. Включив в файл заданий cron строку

```
0,20,40 * * * * cd /usr/local/bin; ./chkrootkit lkm 2>&1 | mail -s "LKM search for HostName"
root@AdminHost
```

вы обеспечите проверку наличия скрытых в системе процессов с передачей отчетов по электронной почте на адрес root@AdminHost.

С помощью теста sniffer вы можете увидеть в своей сети компьютеры, интерфейсы которых работают в режиме захвата пакетов, что может говорить о сборе трафика с помощью анализатора протоколов. Включив в список заданий строку

```
1,5,11,16,21,26,31,36,41,46,51,56 * * * * cd /usr/local/bin; ./chkrootkit sniffer 2>&1 | mail
-s "Packet sniffer search result for HostName" root
```

вы обеспечите проверку наличия в сети собирающих пакеты интерфейсов с интервалом в 5 минут. Отчеты о результатах проверки будут передаваться локальному пользователю root по электронной почте. Такого же результата можно добиться с помощью строки задания

```
1,5,11,16,21,26,31,36,41,46,51,56 * * * * /usr/local/bin/ifpromisc 2>&1 | mail -s "Packet
sniffer search result  for HostName" root
```

Отмечу, что в режим сбора пакетов интерфейс могут переводить не только анализаторы протоколов, но и ряд других программ. Например, на станции, где используются программы Snort, p0f, iplog и arpwatch, команда ifpromisc будет выдавать следующую строку:

```
eth0: PF_PACKET(/usr/sbin/iplog, /usr/sbin/arpwatch, /usr/sbin/p0f, /usr/sbin/snort-bloat)
```

Однако при появлении дополнительной информации уже возникает повод для настороженности. Например, при активизации программы tcpdump строка для этого же хоста примет вид

```
eth0: PF_PACKET(/usr/sbin/iplog, /usr/sbin/arpwatch, /usr/sbin/p0f, /usr/sbin/snort-bloat, /
usr/sbin/tcpdump)
```