Антивирус ClamAV

1. Зачем нужен антивирус в Linux

Linux считается одной из самых безопасных операционных систем. Она устойчива, ее сетевые сервисы надежны и ... для Linux существует очень мало вирусов. Почему? Давайте подумаем. Представим на некоторое время, что мы — вирусописатели. Для какой операционной системы мы бы написали вирус? Для той, в которой работает на данный момент большинство компьютеров и которая более доступна в плане внедрения вируса? Или для той, которая не так популярна, как первая, и в несколько раз неприступнее? Думаю, мы бы выбрали первый вариант. Вот такой вариант как раз и есть Windows. Начнем с того, что для DOS было написано очень много вирусов, и все они по наследству перешли в Windows. Но система Windows несла в себе не только новые функции, но и новые ошибки, каждая из которых порождала новую волну вирусов. Не успевали в Microsoft закрыть одну "дыру", как появлялась следующая. Чего только стоит дырявый Internet Explorer, через который буквально за 10−15 минут в Интернете может проникнуть в систему целая армия троянов, сетевых червей и прочей нечисти. Windows, с ее передовыми и непроверенными технологиями — отличная цель для вирусописателей. Ведь вирусописатели, в какой-то степени, творческие люди. И им интересно, чтобы их "творение" развивалось. А в Linux развитие вируса пресекает сама операционная система. Предположим, что Linux-пользователь скачал какой-то вирус для Linux. И даже запустил его. Максимум, что может сделать вирус — это повредить файлы в домашнем каталоге пользователя. Ведь для всего остального у него не хватит полномочий. А если вирус запустит пользователь root? Да, вирус в этом случае сможет нанести ущерб системе. Но, скажем так, это единичный случай. Все грамотные Linux-пользователи никогда не запускают ничего подозрительного под пользователем root и вообще ежедневную работу выполняют под обычным пользователем, а под пользователем root выполняют только системно-важные операции — просмотр WWW к ним, как мы знаем, не относится. Да и Linux-браузеры не содержат такого огромного количества "дыр", как IE.

Если вирусов под Linux нет, спрашивается: зачем же тогда нужен антивирус? Антивирус нужен как раз для обеспечения безопасности Windows-машин. Большинство антивирусов для Linux предназначены для установки на шлюзах — машинах, которые предоставляют доступ к Интернету. Установив антивирус на шлюзе, вы сможете контролировать трафик, проходящий через шлюз. Таким образом, вы защитите Windows-машины от проникновения вируса. Охрану ставят на входе, не так ли? Конечно, антивирус на шлюзе — это не панацея. Не нужно рассчитывать, что

он на все 100 % обезопасит вашу сеть. Желательно, чтобы на каждой Windows-машине был установлен отдельный антивирус, работающий в режиме монитора.

В этой главе мы будем рассматривать бесплатный антивирус ClamAV (**http://www.clamav.net**). Почему именно ClamAV, а не какой-нибудь коммерческий антивирус вроде DrWeb или Kaspersky AntiVirus? Коммерческие антивирусы сопровождаются хорошей документацией, в которой вы разберетесь и без моих комментариев, да и не хочется отбирать хлеб у службы поддержки коммерческих антивирусов.

2. Установка ClamAV

Для работы ClamAV нужно установить три пакета (если пакетов нет в составе вашего дистрибутива, то их можно скачать с сайта **www.clamav.net**):

- clamav — сканер;
- clamav-db — антивирусная база данных;
- clamd — демон Clam (в новых версиях Clam демон clamd входит в состав пакета clamav).

Сразу после установки нужно установить соединение с Интернетом (если оно еще не установлено) и выполнить обновление антивирусной базы данных:

```
# /etc/init.d/clamd start
# freshclam
```

Первая команда запускает демон Clam, чтобы у `freshclam` (выполняет обновление базы данных) была возможность сообщить демону об удачном обновлении баз данных.

> ***Примечание***
>
> Команды `clamd` и `freshclam` нужно запускать от имени пользователя root. Напомню, что для этого не нужно входить в систему как root: достаточно использовать команды `su` или `sudo`.

3. Проверка файловой системы

Сомневаюсь, что в вашей файловой системе будут вирусы (не забываем, что мы используем одну из самых безопасных операционных систем), но все же лучше запустить сканер:

```
# clamscan -r /
```

Эта команда проверит всю файловую систему. Если нужно проверить только отдельный каталог, то вместо `/` укажите имя каталога.

4. Прозрачная проверка почты

Сейчас мы настроим прозрачный почтовый антивирус. Почтовый антивирус чрезвычайно актуален, ведь большинство так называемых *сетевых червей* распространяются именно с помощью электронной почты.

Конечно, антивирус ClamAV можно использовать и в режиме обычного сканера, но наиболее интересен он в режиме почтового антивируса. Чуть раньше было сказано, что данный антивирус является прозрачным. Почему прозрачным? Обычный почтовый антивирус "прикручивается" к MTA-агентам путем внесения изменений в их конфигурационные файлы. Агент MTA "знает", что прежде чем передать письмо, его нужно проверить, вызвав прописанный в конфигурационном файле антивирус. Прозрачный антивирус действует независимо от MTA-агента. Более того, MTA-агент даже не подозревает о его существовании. Это очень удобно, хотя бы потому, что нам не нужно изменять конфигурацию MTA-агента. Вы когда-нибудь "прикручивали" антивирус, например, к sendmail? Если нет, то обязательно попробуйте, когда у вас будет свободное время. После этого вы оцените технологию "прозрачности" ClamAV.

Но простота внедрения — это не единственное преимущество ClamAV. Представьте, что у вас есть почтовый сервер, на котором вы развернули почтовый антивирус. Все бы хорошо — почта ведь проверяется. Но! Ведь у ваших сотрудников есть ящики не только на локальном почтовом сервере. Наверняка найдется несколько человек (если не подавляющее большинство), у которых есть почтовые ящики на бесплатных почтовых серверах, например на **Mail.ru**. В этом случае вирус может попасть в вашу сеть, когда пользователь получает почту с сервера **Mail.ru**. Наш антивирус будет бессилен, поскольку он контролирует только наш локальный сервер. Правильно настроенный ClamAV будет проверять абсолютно все почтовые соединения, т. е. соединения с 25 и 110 портами любых серверов.

Сам ClamAV является обычным антивирусом, а "прозрачным" его делает сервер P3Scan, скачать который можно по адресу **http://sourceforge.net/projects/p3scan/.**

Антивирус у нас уже установлен и работает, поэтому можно приступить к настройке P3Scan. Работать все будет так: iptables брандмауэра будет перенаправлять пакеты на порт, на котором запущен P3Scan. После этого начинает работать ClamAV, которому P3Scan передает для проверки почту. Неинфицированная почта будет отправлена клиенту.

Теперь, собственно, настройка. Отредактируйте файл /etc/p3scan/p3scan.conf следующим образом:

```
virusregexp = .*: (.*) FOUND
scanner  = /usr/bin/clamdscan --no-summary -i
scannertype = basic
```

Если нужно, измените путь к ClamAV.

Все, что осталось сделать — это создать правило перенаправления POP3-трафика на порт 8110 (на этом порту работает P3Scan):

```
# iptables -t nat -A PREROUTING -p tcp --dport 110 -j REDIRECT --to 8110
```

5. Проверка Web-трафика

Почта — это не единственный способ распространения сетевых червей и прочей нечисти. Очень много вирусов распространяются по WWW, поэтому нам нужно (на шлюзе) перехватить WWW-трафик, проверить его антивирусом и, если трафик "чистый", передать его пользователю.

Работать прозрачный антивирус Web-трафика будет на базе уже установленного и настроенного прокси-сервера Squid — Squid будет получать запрашиваемый пользователем по WWW файл и с помощью программы Viralator передавать его антивирусу. Кроме программы Viralator, есть и другие программы, которые можно использовать для этой цели, но работать с Viralator проще. Также можно организовать передачу файлов между прокси-сервером и антивирусом с помощью стандартных редиректоров Squid, но они не всегда работают корректно, поэтому мы их использовать не будем. Кроме программы Viralator нам понадобится запущенный на шлюзе Web-сервер Apache — через него и будет запускаться сценарий Viralator.

Скачать программу Viralator можно на сайте **http://viralator.sourceforge.net/**.

Теперь можно приступить к настройке. Настройки Squid рассматривать не будем — с ними мы уже знакомы. На уже настроенный Squid нужно установить squidGuard и отредактировать его конфигурационный файл /etc/squid/squidGuard.conf (листинг 1).

Листинг 1. Конфигурационный файл etc/squid/squidGuard.conf

```
# Путь к базе squidGuard и журналам
dbhome /usr/share/squidGuard-1.2.0/db
logdir /var/log/squidGuard

dest files {
expressionlist files-to-check.reg
  }
  acl {

# 10.0.0.1 — это IP Web-сервера, на котором установлен Viralator
default {
pass !files all
redirect
http://10.0.0.1/cgi-bin/viralator.cgi?url=%u
   }
  }
```

Этот конфигурационный файл заставляет squidGuard передавать файлы, имена которых соответствуют регулярному выражению из файла files-to-check.reg, сценарию viralator.cgi, расположенному на Web-сервере.

Нам нужно создать файл /usr/share/squidGuard-1.2.0/db/files-to-check.reg и поместить в него следующее регулярное выражение:

```
(\.exe$|\.bat$|\.zip$|\.bin$|\.sys$|\.rar$)
```

Как несложно догадаться, эта строка задает типы файлов для проверки — такие типы файлов потенциально могут содержать вирусы. Можете отредактировать приведенную строку так, как считаете нужным.

Мы пока что связали сценарий Viralator со squidGuard, но не связали сам squidGuard со Squid. Для этого откройте файл /etc/squid/squid.conf и добавьте в него следующие строки:

```
redirector_bypass on
redirect_program /usr/local/squidGuard/bin/squidGuard

# максимальное количество копий squidGuard в памяти
redirect_children 20
redirector_access deny SSL_ports
redirector_access deny localhost
```

Теперь нужно настроить Apache. Откройте его конфигурационный файл /etc/httpd/conf/httpd.conf и отредактируйте следующие директивы:

```
# указываем IP нашего Web-сервера
Listen 10.0.0.1:80
ServerName 10.0.0.1
```

Не забудьте после этого запустить Apache.

Теперь приступим непосредственно к настройке программы Viralator. Сценарий viralator нужно распаковать в каталог /var/www/cgi-bin, после чего изменить владельца и права доступа сценария:

```
# chown apache:apache /var/www/cgi-bin/viralator.cgi
# chmod +x /var/www/cgi-bin/viralator.cgi
```

Сценарий Viralator требует дополнительный Perl-модуль LWP. Для установки этого модуля нужно ввести команду:

```
# perl -MCPAN -e shell
```

А когда увидите приглашение **cpan>**, введите команду: `install LWP`.

После этого перейдите в каталог /var/www/cgi-bin (именно в него вы должны были распаковать архив с viralator). В этом каталоге найдите подкаталог etc, а в нем — подкаталог viralator — скопируйте его в каталог /etc. После чего удалите каталог etc из каталога /var/www/cgi-bin.

Почти все готово. Осталось только отредактировать конфигурационный файл Viralator — /etc/viralator/viralator.conf (листинг 2).

Листинг 2. Файл /etc/viralator/viralator.conf

```
servername -> 10.0.0.1       # IP-адрес Web-сервера
antivirus -> CLAMAV          # мы используем ClamAV
virusscanner -> clamscan     # так называется программа-сканер
scannerpath -> /usr/bin      # а это путь к сканеру
viruscmd -> --remove         # опция сканера для удаления вирусов
```

```
alert -> FOUND        # сообщение сканера о том, что найден вирус
downloads -> /var/www/html/downloads       # этот каталог нужно создать
downloadsdir -> /downloads
default_language -> english.txt            # язык по умолчанию (русского нет)

# остальное можно не изменять
scannersummary -> true
popupfast -> false
popupback -> false
popupwidth -> 600
popupheight -> 400
filechmod -> 644
BAR -> bar.png
PROGRESS -> progress.png
```

Создайте каталог downloads и установите права доступа:

```
# mkdir /var/www/html/downloads
# chown apache:apache /var/www/html/downloads
# chmod 777 /var/www/html/downloads
```

Все! Теперь машины клиентов нужно настроить на использование нашего прокси-сервера (10.0.0.1, порт 3128) и приступить к тестированию!

6. Клиентский антивирус

Какой антивирус лучше всего установить на компьютерах нашей сети, которые работают под управлением Windows? Несмотря на то, что есть Windows-версия ClamAV, я бы порекомендовал антивирус Касперского, поскольку ClamAV не всегда эффективно справляется с некоторыми угрозами. ClamAV, установленный на шлюзе, "отсеет" бóльшую часть вирусов, а с теми, которые ClamAV пропустит, справится антивирус Касперского.