logcheck

Пакет **logcheck** предназначен для автоматической проверки системных журналов на предмет обнаружения опасных событий (security violations) и необычных действий. Logcheck использует программу logtail, которая помнит позицию последнего чтения журнального файла и при последующем запуске начинает обработку с этой позиции. Пакет **logcheck** построен на основе сценария frequentcheck.sh из состава брандмауэра Trusted Information Systems[1] Gauntlet™ с разрешения авторов.

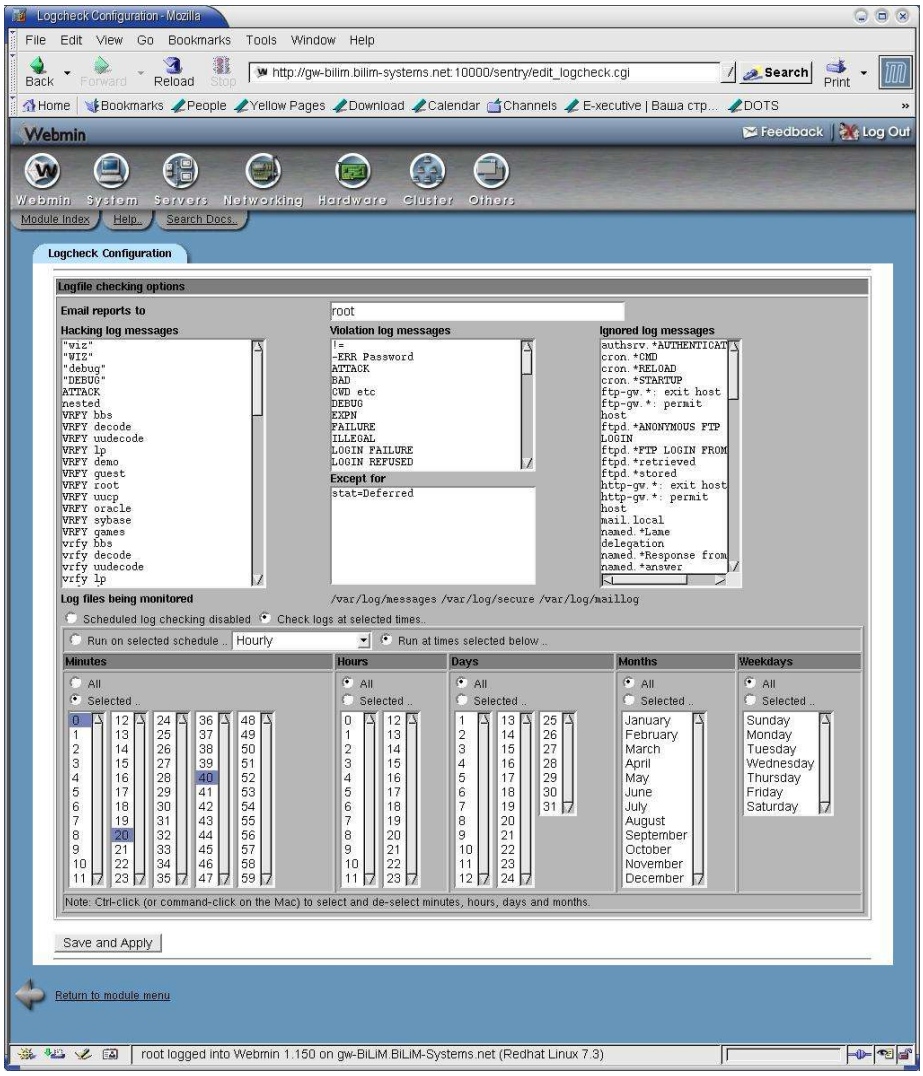

Рисунок 1 Интерфейс Webmin для настройки LogCheck

Аудит журнальных файлов системы весьма актуален с точки зрения безопасности. Что может быть важнее для администратора, чем своевременное получение информации о возникновении в системе проблем, которые могут в дальнейшем осложнить ее функционирование или совсем блокировать нормальную работу системы.

Практически все современные реализации Unix поддерживают тип сообщений syslog для передачи отчетов и обеспечивают достаточный уровень гибкости, предоставляя администратору информацию о всех важных событиях в системе. Программа **logcheck** автоматически выполняет работу по аудиту системных процессов на основе журнальных файлов и показывает администратору проблемные точки в системе.

Работа программы logcheck основана на периодической проверке журнальных файлов с целью обнаружения опасных и необычных ситуаций в работе системы. При обработке журнальных файлов используются два основных метода уведомления администратора:

1) генерация отчетов обо всех событиях, заданных администратором ключевыми словами;

2) генерация отчетов обо всех событиях, которые администратор не счел нужным игнорировать; такие события также задаются ключевыми словами.

Такая обработка журнальных файлов обеспечивает гарантию того, что важная и интересующая вас (заданная ключевыми словами) информация не будет оставлена без внимания.

Сценарий **logcheck** следует запускать по крайней мере один раз в час с использованием демона cron. Все обнаруженные события указываются в сообщении, передаваемом администратору по электронной почте.

Программа распространяется с базовым набором ключевых слов для различных вариантов ОС, но вы можете создать свои наборы ключевых слов для их поиска в журнальных файлах системы. Редактировать файлы ключевых слов можно с помощью привычного вам редактора. Существует модуль Security Sentries для редактирования ключевых слов и режима работы logcheck в программе Webmin. Интерфейс этого модуля показан на рисунке 1.

Пакет Logcheck включает несколько файлов:

logcheck.sh – основной сценарий, используемый для просмотра журнальных файлов и генерации сообщений для администратора.

logtail – исполняемый файл, который сохраняет информацию о позициях журнальных файлов, на которых была завершена обработка при прошлом запуске сценария. При каждом запуске обработка файла начинается с сохраненной позиции, что позволяет существенно ускорить процесс анализа и снизить загрузку системы. Особенно важна эта возможность при обработке больших журнальных файлов на маршрутизаторах и межсетевых экранах. Периодическое обновление журнальных файлов утилитой logrotate, поэтому при переходе к новому файлу счетчики смещения автоматически сбрасываются.

logcheck.hacking – содержит список ключевых слов, по которым идентифицируются возможные атаки на вашу систему. Этот файл не требуется редактировать, если только вы не сочтете нужным добавить в него новые ключевые фразы, которые обнаружите в своих журнальных файлах после атаки. Включенный по умолчания список содержит ключевые фразы, генерируемые сканерами

[1] http://www.tis.com

безопасности и программой sendmail (при некорректном синтаксисе строки адреса). При обнаружении в журнальном файле заданных ключевых слов будет генерироваться предупреждение с заголовком **ACTIVE SYSTEM ATTACK**

logcheck.violations – содержит ключевые слова для идентификации системных событий, которые представляются нежелательными. Связанные с ключевыми словами из этого файла появляются в отчете под заголовком **Security Violations**.

logcheck.violations.ignore – этот файл содержит ключевые слова, при наличии которых запись из журнального файла не включается в раздел отчета **Security Violations**. Покажем это на примере обработки строк:

```
Feb 28 21:00:08 nemesis sendmail[5475]: VAA05473: to=crowland, ctladdr=root (0/0),
delay=00:00:02, xdelay=00:00:01, mailer=local, stat=refused
Feb 28 22:13:53 nemesis rshd: refused connect from hacker@evil.com:1490
```

Первая запись описывает достаточно часто встречающуюся ситуацию, когда удаленный транслятор по каким-то причинам отказался от организации соединения с вашей системой (**stat=refused**). Во второй записи говорится, что некто (hacker@evil.com) безуспешно пытался инициировать сессию **rsh** на вашей машине – это, скорей всего, плохо. Файл **logcheck.violations** включает ключевое слово **refused** и обе записи должны были появиться в отчете. Однако мы можем избавиться от первой записи (таких записей может быть весьма много и они не содержат актуальной информации), поместив в файл **logcheck.violations.ignore** ключевые слова

```
mailer=local, stat=refused
```

В результате отчет будет содержать лишь вторую запись из журнального файла.

При включении ключевых слов в файл **logcheck.violations.ignore** следует соблюдать осторожность. Слишком короткая фраза, на основании которой запись из журнального файла будет пропущена, может привести к тому, что вы не увидите достаточно важных событий.

logcheck.ignore – этот файл содержит ключевые слова, при наличии которых в записях журнального файла не включаются ни в один раздел. Все строки журнальных файлов, которые не содержат ключевых слов из этого файла и не были включены в другие разделы отчета, помещаются в раздел **Unusual System Activity**. Следует с осторожностью подходить к выбору ключевых фраз для этого файла и не включать к него слишком коротких ключей поиска.