Глава 3: Редактирование и тестирование sudoers

Если sudo не может разобрать /etc/sudoers, она не будет работать. Если вы используете sudo для получения привилегий суперпользователя на сервере, вам может быть отказано в использовании привилегированных команд. Исправление sudoers так же является привилегированной командой. Это плохое положение дел. Не стоит в него попадать. Sudoers должен содержать допустимый синтаксис. Sudo включает специальный инструмент visudo предназначенный для редактирования sudoers.

Visudo защищает вас от очевидных ошибок в sudoers. Он блокирует доступ к sudoers таким образом чтобы только один человек мог произвести изменение, в конкретный момент времени *(п.п: будем называть это "исключительной блокировкой")*. Visudo открывает копию файла в текстовом редакторе. При сохранении файла, visudo производит его анализ и проверяет соответствии грамматике sudo. Если ваш новый файл sudoers синтаксически верен, visudo копирует новый файл в /etc/sudoers. Однако, следует помнить, что "синтаксически верный" не означает "делает то что вы хотели".

По умолчанию, visudo использует редактор vi. Хотя всем системным администраторам следует владеть vi, это не означает, что у вас нет иной возможности. Visudo лояльно относится к переменной окружения $EDITOR, а следовательно, вы можете использовать любой из привычных вам редакторов. Установите необходимый вам редактор и мы переходим к редактированию sudoers.

Создание /etc/sudoers

Хотя большинство операционных систем включают образец или дефолтный файл sudoers, имеющий достаточное количество примеров, в целях обучения мы создадим политики sudoers с нуля.

Переместите исходный файл sudoers в надёжное место. При запуске, visudo создаст новый файл.

#visudo

Для начала, создадим очень простой файл sudoers, предоставив вашей учётной записи полные права на сервер. Вот, thea предоставляет себе неограниченный доступ посредством sudo:

thea ALL=ALL

Сохраним файл и выйдем. При наличии такого простого правила, разрешающего одному пользователю полный доступ к машине, редактор должен завершить работу без ошибок, а visudo должно установить правила. *(п.п: да, конечно, если вы не ошиблись в имени пользователя, то всё будет хорошо...)*

Теперь, в качестве обучения, повредим sudoers (пользователи Ubuntu и Apple, надеюсь у вас есть пароль root?). Запустите visudo и потыкайте клавиши, чтобы создать мусорную строку в нижней части файла. Сохранимся и выйдем. Вы должны увидеть следующее:

#visudo >>>/usr/local/etc/sudoers:syntax error near line 3 <<<

What now?

Если вы нажмёте 'e', visudo вернёт вас в текстовый редактор для исправления вашей проблемы. Перейдите к указанной строке и посмотрите что там происходит. Удалите весь мусор и visudo позволит вам выйти из текстового редактора и установит правила.

Чтобы отказаться от изменений и сохранить прежние правила sudoers, нажмите 'x'. Старый рабочий файл лучше чем новый не рабочий. Я несколько раз делал это в процессе обучения sudo, так что на данном этапе не стоит сильно волноваться.

Если вы нажмёте 'Q' вы установите повреждённый файл в качестве /etc/sudoers. Если sudo не может разобрать /etc/sudoers, он немедленно завершает работу. Нажатие 'Q' приведёт к нарушению работы sudo, вплоть до тех пор, пока вы не войдёте в систему как root и не исправите проблему. Не следует использовать эту клавишу. Результат скорее всего вам не понравится.

Если вы забыли ключевые клавиши, введите знак вопроса - visudo выдаст вам возможные варианты.

Всегда помните, что "правильный" файл sudoers не всегда является "полезным" файлом sudoers. Пустой sudoers, запрещающий все привилегии для всех - является верным и разбирается весьма быстро. Так же, visudo позволяет использовать файл sudoers в котором каждое правило определяет пользователей и команды на системе или сервере отличном от

локальной системы. Если вы создаёте файл sudoers для вашей сети, я настоятельно рекомендую использовать последнее правило дающее разрешение вашей учётной записи на право работать с visudo. Если даже всё остальное будет ошибочно, вы, хотя бы сможете изменять правила.

thea ALL = /usr/sbin/visudo

Помните, что sudo обрабатывает правила по порядку и побеждает последнее совпадающее правило. Поэтому размещайте правило спасения в самом конце файла.

Тестирование sudoers

Итак, вы написали свою первую политику безопасности в sudoers. Сейчас она легко читается - имеется все две строки: запись полного доступа и аварийный доступ к visudo. Однако, когда ваши политики становятся более сложными, достаточно не просто сказать может ли пользователь получить конкретный доступ.

Для просмотра своих привилегий, пользователи могут использовать флаг sudo -l.

$sudo -l

Password:

User thea may run the following commands on this host:

(root) ALL

(root) /usr/sbin/visudo

$

Когда пользователь thea вводит пароль, он видит с какими командами может работать. Вывод может показаться немного странным, но он должен быть знакомым. Это стандартная запись sudoers в которой удалены имя пользователя и имя хоста. Помните, что если вы не укажите имя пользователя в sudoers, sudo выполнит команду как root. Это может оказаться более очевидным в более сложном примере:

$sudo -l

User thea may run the following commands on this host:

(root) ALL

(oracle) ALL

(root) /usr/sbin/visudo

thea может выполнять все команды как root, все команды как пользователь oracle, а visudo - как root.

Итак, пользователю удобно проверить свои привилегии, но как насчёт системного администратора? Как быть уверенным, что политики sudoers работают именно так, как было задумано? Используйте флаг -U совместно с флагом -l для указания пользователя.

#sudo -U mike -l

User mike is not allowed to run sudo on www.

Только суперпользователь и пользователи которые могут использовать ALL команды на текущем хосте могут использовать ключ -U. Со своей, непривилегированной учётной записью, я могу проверить только свой собственный доступ. Sudo видит, что thea обладает политикой ALL, следовательно он может просматривать мои права доступа. В противном случае, ему придётся выполнить sudo -u mike sudo -l, что выглядит глупо.

На протяжении книги мы будем использовать sudo -l, чтобы видеть, как сложные политики sudoers расширяются в видимые пользователем правила. Я рекомендую использовать флаг -U непосредственно после внесения изменений, чтобы проверить права доступа пользователя, прежде, чем сообщать пользователю о предоставление запрошенных им привилегий.