УДК 004.3

Усиления безопасности appache web сервера

Ашихин В.А.группа 11Р

Усиления безопасности Appache Web сервера.Appache - это программа, которая исполняет функции http-сервера. Именно с ее помощью и будет функционировать вебсервер. Эта программа исполняет все необходимые функции, под ее руководством работает большинство ресурсов сети. Согласно результатам некоторых отчётов, более 70% контингента, опубликованного в сети Интернет, поддерживается сервером Appache, что делает его более широко используемым.Apppache - это проект Apache Software Foundation, цель которого предоставить защищённый, эффективный и расширяемый сервер, предоставляющий службы HTTP, которые отвечают современным HTTP- стандартам.

Первым шагом что необходимо сделать, скрыть информацию о версии Appache. По умолчанию многие сборки Appache готовы рассказать всему свету, какой они на самом деле версии, в придачу версию операционной системы, на которой собственно и крутится Appache и даже какие модули Appache установлены на сервере. Злоумышленникам это очень хорошо помогает как в процессе исследования сервера, так и самого взлома.Две записи, которые необходимо добавить или исправить в файле httpd.conf:

ServerSignature Off

ServerTokens Prod

ServerSignature появляется внизу страниц, сгенерированных apache, таких как 404, списки каталогов.Запись ServerTokens используется в заголовках HTTP ответа. Изменив значение на Prod, мы получим следующий заголовок HTTP ответа:*Server: Appache*

Appache должен запускаться с отдельным пользовательским акуатом.

Некоторые сборки appache запускаются как пользователь nobody. Таким образом, если Appache и почтовый сервер запущены от имени nobody, то

удачная атака на Appache приведет к компрометации и почтового сервера, и наоборот. Следуюшим шагом что необходимо сделать,выключить просмотр директорий, то есть не даем возможность просматривать любому посетителю содержимое директорий вашего сайта, включая PHP скрипты и другие служебные файлы. Делается это при помощи директивы Options внутри тэга Directory. Установим значение для Options в None или -Indexes.

Options -Indexes.

Запуск mod_security.В папке */usr/local/apache2/conf/rules/* находится конфигурационный файл *modsecurity_crs_10_config.conf* с базовыми настройками модуля ModSecurity.

ModSecurity – модуль Apache, добавляющий возможности обнаружения и предотвращения вторжения на Web сервер.Модуль подобен IDS системе, которая используется для анализа сетевого трафика, за исключением того, что mod_security работает только на HTTP уровне. Модуль позволяет анализировать действия, обычные с точки зрения HTTP протокола, но трудные для анализа классическими IDS системами. ModSecurity перехватывает запросы к Web-серверу, на котором он установлен. HTTP запрос от клиента сначала обрабатывается ModSecurity. Модуль сравнивает запрос со своими правилами и, если запрос не блокируется, передает его на обработку Web-серверу. ModSecurity также может контролировать ответы Web-сервера, т.е. после формировании страницы ответ обрабатывается модулем и, в соответствии с правилами, блокирует или разрешает прохождение ответа.Основные функции которые выполняет ModSecurity:

Простое фильтрование

Фильтрование, основанное на регулярных выражениях

Проверка URL кодировки

Проверка Unicode кодировки

Предотвращение атаки «Null byte»

Ограничение загрузки памяти

Маскировка сервера

Контроль пользователей блога.Обычно настройки блога позволяют зарегистрироваться на нем любому пользователю. Тут важно предоставлять каждому из них минимально необходимый уровень доступа. Если у какого-то пользователя достаточно большие права доступа, то он может использовать ваш сайт не по назначению. Поэтому необходимо следить за тем, какие права доступа у каждого из зарегистрированных пользователей, и корректировать их, если это нужно.При введении неправильного логина или пароля при входе в админ панель блока,выдается сообщение об ошибке. Это сообщение помогает хакерам в их нелегкой работе по взлому сайта. Поэтому от вывода сообщений об ошибке доступа стоит отказаться вообще. Для этого в файл functions.php добавляется строчка:

add_filter('login_errors',create_function('$a', "return null;"));

Уменьшить значение Timeout.По умолчанию значение директивы Timeout составляет 300 секунд. Уменьшение этого значения позволяет снизить воздействие потенциальных DOS атак.В Apache есть несколько директив, которые позволяют уменьшить размер запроса, что также может быть полезным для предотвращения некоторых видов DoS атак.Лучше всего начать с директивы LimitRequestBody. По умолчанию ограничение отсутствует. Если использовать загрузку файлов размером не более 1 МБ,то нужно установить следующее значение:LimitRequestBody 1048576.Некоторые другие директивы, на которые следует обратить внимание это LimitRequestFields, LimitRequestFieldSize и LimitRequestLine. Этим директивам по умолчанию присвоены приемлемые для большинства серверов значения, но более тонкая настройка никогда не помешает.

В Appache есть несколько настроек, которые позволяют изменить число одновременно обрабатываемых запросов. MaxClients - максимальное число дочерних процессов, которые буду созданы для обслуживания запросов. Это значение зависит от объема оперативной памяти вашего сервера.

Другие директивы, такие как MaxSpareServers,MaxRequestsPerChild, а на Appache2 ThreadsPerChild, ServerLimit, and MaxSpareThreads важны и их

необходимо настроить в соответствии с вашей операционной системой и аппаратными возможностями.

Борьба со спамом.Существуют программы автоматической рассылки спама на блоки. Они запускаются на других серверах, и шлют спамовые комментарии по списку, куда только можно. Для того чтобы перекрыть дорогу таким «комментаторам», надо добавить в файл .htaccess блок кода, который проверяет, отправлен ли комментарий с нашего сайта. И если это не так, блокирует доступ к блоку.

```
#Stop spam
<IfModule mod_rewrite.c>
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\. [NC]
RewriteCond %{HTTP_REFERER} !.*mysite\. [OR,NC]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*) – [F,L]
</IfModule>
```

Запуск Apache в Chroot среде. Создание замкнутого пространства с помощью утилиты chroot является эффективным средством для более безопасного запуска программ. При этом зона действия этих программ ограничивается частью общего дерева каталогов. Предположим, что нужно создать замкнутое пространство для работы условной программы convict. Ограничим зону ее действия частью дерева каталогов /usr/local/convict. Создание замкнутого пространства заключается в том, что программа convict сможет “видеть” только этот каталог и файлы в подкаталогах этого каталога.

Chroot позволяет вам запускать программы в собственном изолированном пространстве. Это предотвращает возможность того, что взлом одного сервиса повлечет за собой дальнейшую компрометацию сервера.

Достаточно простые меры, но в то же время весьма эффективные. Не следует ими пренебрегать, и сайт Ваш будет в большей безопасности.

Список литературы

1. Скотт Хокинс:Администрирование Web-сервера Apache. Издательство: Диалектика, 2001 г. - С. 143-152.

2. М. Арнольд. Безопасность сервера. Издательство: «Лори», 2002,С.59-