СЕРВЕР АРЕНДЫ WWW-ПРОСТРАНСТВА

Ю.В. Шевчук, СВ. Бурчу

Со времени своего первого шага по глобальной сети Интернет каждый человек мечтает создать и разместить в Сети свой сайт. Но не у каждого человека есть свой собственный сервер с постоянным выходом в Сеть, чаще всего такая возможность есть у людей тесно связанных с компьютерами и Интернет. Однако обычный человек такой возможности не имеет. Услуга аренды WWW-пространства позволяет решить данную проблему. Пользователю уже не нужно обладать своим собственным сервером с постоянным выходом в Сеть, постоянно включенным и под постоянным присмотром квалифицированного системного администратора, которому нужно платить зарплату. К тому же чаще всего сервер, на котором осуществляется аренда, располагают более удачно (чем это бывает для обычных абонентских подключений) в смысле скорости доступа к внешнему Интернету. Поэтому данная услуга весьма привлекательна для широкого круга лиц.

На раннем этапе становления Интернета возможности (размещение статичных документов, доступ к арендованному пространству по протоколу FTP и другое), предоставляемые данной услугой вполне соответствовали потребностям пользователей. Но за прошедшее с тех пор время многое изменилось: получили широкое распространение технологии создания Интернет-сайтов с динамическим содержанием; пользователи требуют размещения на сервере аренды не только готовых документов, но и программ и баз данных. Сеть развивается, появляются клиенты, которых статические сайты уже не устраивают и которым нужны дополнительные возможности, например для создания специализированного сетевого магазина.

Предоставление услуг аренды на этом новом уровне приводит к тому, что обычных средств контроля ресурсов сервера и его безопасности недостаточно. Предоставляя пользователю возможность исполнения программ, создатели данной услуги рискуют безопасностью самой системы и неучтённым расходом ресурсов (имеется в виду трафик отдельного пользователя). Пользователь, используя данные ему возможности, способен сильно увеличить общие для всех пользователей расходы на трафик. Так же возможно использование недобросовестным пользователем уязвимостей в программном обеспечении для получения контроля за всей системой.

Прежде всего, на этом новом уровне требуются новые механизмы контроля использования ресурсов сервера пользователями. Кроме того, требуется продуманная схема обеспечения безопасности сервера с позиций "недоверия к пользователю". Реализации такого подхода в посвящена данная работа.

Сервер аренды базируется на основе операционной системы (ОС) Linux.

В возможности сервера аренды входит:

- Доступ к арендуемому пространству через SSH.
- Возможность использования баз данных через Mysql.
- Возможность использования технологий CGI (Perl, PHP) для создания сайтов с динамическим содержанием.

Для управления ресурсами сервера аренды используются следующие механизмы:

- Для контроля дискового пространства используется Quota.
- Для контроля процессора и памяти используется Linux PAM.
- Для контроля трафика пользователей используется собственный механизм SAcct (Socket Accounting).

SAcct контролирует трафик каждого пользователя сервера аренды. В операционной системе Linux очень трудно проконтролировать все сетевые соединения на уровне пользователя. Гораздо удобнее это сделать на уровне ядра операционной системы, что и реализовано в SAcct. Однако на данном уровне возникает проблемы вывода данных из ядра ОС. Возникла необходимость создания удобного инструмента для вывода данных из ядра ОС. Обычно программисты используют для вывода данных syslog, что подразумевает хранение данных в текстовом формате, который удобен для чтения, но неоптимален по количеству занимаемого дискового пространства. Более выгодным вариантом для хранения данных оказался бинарный формат. Размеры сохраненных данных между выводов в syslog и данным форматом различаются примерно в 50 раз. Новый механизм позволяет вывести данные из ядра операционной системы в любой нужный файл минуя пользователя.

Для обеспечения безопасности сервера аренды используются:

- Возможности дистрибутива ОС Linux.
- Система GrSecurity.

GrSecurity исправляет некоторые архитектурные недостатки ОС Linux, что позволяет во многих случаях избежать использования широко распространенных в сети exploit (exploit - программа, использующая какую-либо уязвимость в программном обеспечении для выполнения им непредусмотренных программистом действий либо для его неработоспособности).

- Собственная система слежения за происходящим в операционной системе STrack.

STrack (Syscall Tracking) позволяет отслеживать системные вызовы в ОС Linux. Системные вызовы - единственный механизм управления операционной системой. Возможность отследить некоторое множество системных вызовов для всех процессов системы позволит иметь под наблюдением весь процесс работы сервера аренды. В случае вторжения STrack даст возможность провести детальное расследование и быстро найти и исправить уязвимость в системе. Все данные сохраняются в бинарном формате. Механизм вывода данных из ядра ОС аналогичен SAcct.

На сегодняшний день сервер аренды находится в тестовой эксплуатации. Компонента SAcct реализована и успешно работает, компонента STrack находится в стадии доработки и оптимизации, остальные успешно внедрены и эксплуатируются.