Визитка

ЮРИЙ ДЕНИСОВ, начальник технического отдела одного из провайдеров г. Владимира. Сфера профессиональных интересов: сетевые технологии, проектирование распределенных сетей передачи данных, развертывание телематических сервисов, биллинговые системы

Атаки из сети Интернет
Веб- и DNS-серверы

В статье рассматриваются основные виды угроз, которым подвергаются веб- и DNS-серверы, а также методы уменьшения рисков данных угроз

Веб-сервер

Веб-сервер – это приложение, формирующее информацию, доступную по протоколу HTTP.

Защита веб-сервера должна складываться из нескольких компонентов.

Прежде всего, это устранение уязвимостей в серверном ПО. Здесь рекомендации простые. Вовремя устанавливаем заплатки и внимательно настраиваем сервер. Я для себя выбрал такой подход – ни одна строка в конфигурации не должна вызывать сомнения (каким должен быть ее аргумент, и для чего она вообще предназначена). Сделано это потому, что файл конфигурации, к примеру, того же Apache довольно велик, и, если вы не знакомы с какой-либо частью конфигурации, нет гарантии, что она правильно настроена. Конечно, в большинстве случаев для запуска сервера требуется изменение всего нескольких строк, но насколько такая конфигурация будет оптимальна и безопасна? Кроме того следует по возможности избегать подключения модулей, не требующих для работы сервера, – некоторые из них могут создать дополнительные дыры и уязвимости.

Грамотно написанный веб-сайт, не допускающий его взлома. Этот вопрос выходит за рамки данной статьи, поэтому доверим его рассмотрение специалистам в области сайтостроения.

Грамотно настроенный сервер, не допускающий даже в случае взлома сайта (а такое все же возможно) потери информации на самом сервере, ее утечки либо изменения. Самое важное здесь – не допустить запуска сервера под пользователем root. Некоторых это прельщает, поскольку снимает лишние хлопоты с настройкой прав доступа к ряду файлов и каталогов (действительно, пользователю root доступно все).

Однако данный процесс будет иметь неограниченные права, а значит, в случае взлома у хакера не будет преград для дальнейшей деятельности.

Кроме того, для каждого виртуального хоста необходимо настройкой сервера прописать его корневой каталог, выше которого он подняться не сможет. Например, для сервера apache это будет директива DocumentRoot.

Если на вашем сервере работает несколько виртуальных хостов, то полезным будет запускать их от разных пользователей. При этом доступ к файлам виртуального хоста должны иметь только их владелец и веб-сервер. В этом случае при взломе одного из сайтов информация на других будет защищена от прочтения.

Если вы используете сервер Apache и вам необходима поддержка PHP, то в этом случае придется использовать PHP не как модуль сервера, а как CGI-приложение. Это связано с тем, что при использовании модуля он всегда запускается от имени того же пользователя, что и сам веб-сервер. Для запуска PHP, как CGI, от имени отдельного пользователя придется включить в сервере поддержку suexec. Механизм установки и настройки такого сервера широко освещен в Интернете, и мы не будем на нем подробно останавливаться.

В общем случае, если у вас все настроено продуманно и не спеша, как правило, волноваться не о чем. Чего не скажешь о другом сервисе – службе доменных имен.

DNS-сервер

DNS – распределенная база данных, использующаяся для получения информации о доменах. Это может быть получение IP-адреса по доменному имени и, наоборот, получение информации о маршрутизации почты и т.д.

По преследуемым целям я бы разделил атаки на DNS-сервер на три основные группы:

Получение прав привилегированного пользователя и выполнение на сервере произвольного кода. Здесь все просто и сложно одновременно. Просто потому, что все, что от вас требуется, – следить за обнаружением тех или иных уязвимостей и своевременное их устранение путем установки заплаток. А сложно потому, что есть вероятность того, что какой-то хакер, обнаружив уязвимость, не будет ее афишировать, а вместо этого начнёт применять на практике. В данном случае сервер попадает под большую угрозу. И, конечно же, целью взлома будет являться не сама служба DNS. Она всего лишь станет средством для проникновения на ваш сервер.

Блокирование работы службы DNS. Злоумышленник пытается тем или иным способом добиться отказа в работе ваших DNS-серверов, при этом его не интересуют никакие конфиденциальные данные вашего предприятия. Эту атаку видно явно, она легко обнаруживается, но гораздо труднее нейтрализуется. Об этом чуть ниже.

Атака с целью «обмана» вашего DNS-сервера, предоставление ему ложной информации с целью последующего взлома пользователей. На мой взгляд, это самая опасная из всех видов атак. Во-первых, вы можете никогда не узнать, что она была произведена. Во-вторых, постфактум крайне сложно (а может, и вообще невозможно) определить инициатора атаки.

Все, что ему будет нужно, это заставить ваш DNS-сервер ассоциировать определенное доменное имя (например, какой-либо платежной системы) с подложным IP-адресом, на котором будет размещен хостинг с подложным сервисом. С помощью этого злоумышленник сможет легко получить интересующую его информацию, например, логин и пароль на данный ресурс.

После этого атака будет свернута, и есть большая вероятность того что вы никогда не узнаете, что при одном из обращений на какой-либо сайт логин и пароль доступа вы вводили не на сам сайт, а на его точную копию. Для того чтобы установить этот факт, придется анализировать горы детальной статистики по трафику и логов прокси-сервера. И это только один из вариантов использования данного вида атак.

В данной статье мы не будем в тонкостях рассматривать принцип взаимодействия хостов по протоколу DNS. Сегодня существует огромное количество литературы, посвященной этому. Я бы хотел остановиться на основных моментах, которые необходимо знать и учитывать каждый раз при проектировании и настройке новой сети.

Итак, рассмотрим некоторые виды атак подробнее.

DDoS-атака

Самая банальная и при этом весьма действенная. Целью её является блокирование работы вашего DNS-сервера. Чаще всего это необходимо в том случае, если ваши серверы хранят файлы определённых зон, работу которых необходимо прервать.

Известно несколько вариантов реализации DDoS-атак, и зачастую невозможно отличить атакующий трафик от полезного. При этом DDoS-атака несет в себе по меньшей мере два негативных момента – замедление обработки поступающих запросов (вследствие высокой загрузки сервера) и забивание каналов передачи данных, к которым подключены DNS-серверы.

Лучшим, на мой взгляд, решением будет доверить хранение файлов ваших зон специализированному хостингу. Он, как правило, имеет гораздо более мощные серверы, каналы передачи данных и распределенную структуру, а, следовательно, более устойчив к атакам.

В случае если этот вариант неприемлем, существуют определенные способы противодействия различного рода атакам из сети Интернет.

Это, во-первых, внедрение локальной системы обнаружения вторжений, а во-вторых, использование онлайн-сервисов, осуществляющих те же самые действия, но при этом освобождающих вас от необходимости установки и настройки весьма сложной системы.

На самом деле это все системы комплексной защиты, и защита DNS-сервера является лишь частным случаем, потому рассмотрению подобных систем мы посвятим одну из следующих статей.

Межсегментная удаленная атака на DNS-сервер

Служба DNS в своей работе использует протокол UDP. Он работает быстрее, чем TCP, и снижает накладные расходы на сервер. Это связано с тем, что UDP-протокол в отличие от TCP не ориентирован на соединение. Отсюда все его плюсы и минусы.

Из минусов можно выделить то, что данный протокол не имеет средств идентификации сообщений. Говоря простым языком, на уровне UDP нельзя гарантировать, что UDP-дейтаграмма, поступившая в ответ на наш запрос пришла действительно от того хоста, с которым мы работаем, и не была сфальсифицирована на другой машине.

Схема работы службы DNS

Теперь рассмотрим схему работы службы DNS с точки зрения конечного пользователя при обращении его на какой-либо веб-сервер. Итак, что происходит, когда пользователь хочет зайти на сайт www.mydomain.com?

Компьютер обращается к DNS-серверу для того, чтобы тот преобразовал доменное имя mydomain.com в IP-адрес, на который он и будет обращаться. DNS-сервер, получив запрос, проверяет свой кеш на предмет нахождения в нем данной записи. Если она есть, то выдаёт компьютеру запрашиваемые данные, если нет, обращается к вышестоящим серверам. Чаще всего это бывает DNS-сервер провайдера, к которому подключена фирма. Кроме того, это могут быть корневые серверы DNS, и далее по цепочке.

В случае, когда кеш сервера пуст, он производит обращение к другому DNS-серверу, который, по его мнению, должен содержать требуемую информацию. Послав запрос, он в течение некоторого времени ожидает ответа.

Для того чтобы ваш DNS-сервер (или конечный хост) принял ответное сообщение за истинное, необходимо, чтобы совпали несколько условий:

- Ответ пришел с того же IP-адреса, на который посылался запрос.
- Ответ пришел на тот же порт, с которого посылался запрос.
- В ответе должно быть указано то же самое имя, что и в DNS-запросе.
- В заголовке DNS должно быть указано то же самое значение идентификатора запроса (ID), что и в самом запросе.

Это означает, что, постаравшись и соблюдя все вышеописанные четыре условия, злоумышленник сможет послать на ваш DNS-сервер UDP-дейтаграмму, содержащую ложные данные, и DNS-сервер примет их за истинные.

Далее он поместит эту запись в свой кеш, и, пока не истечет тайм-аут нахождения этой записи в кеше, сервер будет выдавать на запросы компьютеров вашей сети неправильные данные. Это чревато тем, что вы можете попасть не на свой любимый сайт, а на точную его копию, и ввести в форму свой логин и пароль от сайта. Ваша электронная

почта может быть перенаправлена на другой сервер. Вариантов – море.

Конечно, для хакеров все не так радужно. Остается необходимость определить порт, с которого ваш сервер отправлял запрос, поле ID в запросе и придумать, как отправить UDP-пакет на ваш сервер от нужного IP-адреса (например, используя в качестве адреса отправителя IP-адрес сервера DNS вашего провайдера).

Однако решить эти задачи возможно.

Атаки типа IP-спуфинг указывают на то, что подделать адрес отправителя в ряде случаев оказывается возможным. К тому же UDP-протокол более подвержен этой атаке, нежели TCP, поскольку не имеет встроенных механизмов для предотвращения спуфинга.

Поле ID в запросе узнать тоже весьма реально. В лучшем случае оно будет перебираться, увеличиваясь на единицу при каждом запросе, к какому-либо внешнему серверу. Самым простым способом было бы послать на DNS-сервер какой-либо запрос о домене, подконтрольном злоумышленнику. Но, как правило, такая возможность из внешнего мира закрыта.

В этом случае злоумышленнику необходимо спровоцировать на подобный запрос любой хост из вашей внутренней сети. Один из вариантов работает в случае, если в вашей сети, кроме всего прочего, присутствует корпоративный почтовый сервер, способный принимать письма из внешнего мира.

К примеру, у хакера есть сервер, являющийся первичным для зоны myprivatezone.ru. Все, что ему нужно, – это подключиться на 25-й порт вашего сервера и ввести ряд стандартных команд, провоцирующих ваш сервер на поиск информации о домене myprivatezone.ru. В этом случае ваш почтовый сервер обратится к вашему DNS-серверу, а тот, в свою очередь, не обнаружив в кеше нужной записи, обратится к серверу злоумышленника. С этого момента становится известен примерный диапазон возможных значений ID.

Номер порта, на который будет отправлен ответ, в данном случае это единственный параметр, подбираемый перебором. Еще несколько лет назад данный вид атаки был трудноосуществим именно из-за необходимости посылать большое количество информации с перебором портов получателя (а может, и поля ID в ответе). Но сейчас при наличии каналов в Интернете со скоростью 10, 100 Мбит и более эта задача представляется не такой уж и сложной.

***

Защититься от грамотно построенной подобной атаки с помощью файрвола практически невозможно. Ведь с его точки зрения пакет, пришедший на ваш сервер, будет строго удовлетворять всем правилам и должен быть пропущен системой. Несколько уменьшить риск данной атаки можно, запретив рекурсивные запросы с компьютеров, находящихся во внешней сети. На мой взгляд, оптимальным средством защиты будет система обнаружения вторжений, которая в теории должна достаточно легко обнаруживать и предотвращать подобные типы атак. О ней и пойдет речь в следующей статье. EOF