УДК 681.3:519.2

Т. Радивилова, В. Бушманов
Харьковский национальный университет радиоэлектроники, Украина

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ DNS СЕРВЕРА

T. Radivilova, V. Bushmanov

PROVIDE SECURITY OF DNS SERVER

Существует много проблем защиты информации при работе в сетях общего пользования. DNS (англ. DomainNameSystem) необходим для создания масштабируемых распределенных систем.

Поскольку DNS сервера являются основными поставщиками информации, касающейся корпоративной сети, они всегда будут мишенями для злоумышленников. Пользователь, который обращается из браузера к Web узлу, ожидает получить контент данной страницы. Главной проблемой является достоверность ответа DNS-сервера, которая никак не проверяется, что является слабым звеном данной системы [1]. Подменна DNS ответа, изменение DNS-кеша, создание обманного DNS-сервера, вследствие перехвата запроса, ведет к тому, что пользователи столкнутся с отказом в обслуживании или будут перенаправлены на серверы сомнительного содержания, на которых злоумышленники могут получать доступ к паролям, номерам кредитных карт и другой конфиденциальной информации [2].

Атаки на DNS. Для того чтобы сфальсифицировать данные DNS, злоумышленник может использовать несколько методов для атак [3]:

1) Атака на один хост. Злоумышленник отправляет подложный DNS-ответ атакуемому хосту. Ответ отправляется от имени сервера после того, как хост выслал серверу соответствующий запрос.

2) Атака на все хосты одного DNS-сервера. Злоумышленник отправляет подложный DNS-ответ серверу «А», когда тому требуется найти адрес сервера «Б». Сфальсифицированные данные сохраняются в кэше сервера «А» в течение указанного злоумышленником времени жизни записи, которое может быть очень большим. Действие атаки распространяется на все хосты, использующие сервер «А» в качестве своего DNS-сервера.

3) Атака на DNS-серверы зоны A.some.com. Злоумышленник, от имени первичного сервера A.some.com, производит передачу сфальсифицированной зоны some.com на вторичный сервер A2.some.com. Таким образом злоумышленник введет в заблуждение все DNS-серверы Интернета, которые обратятся к A2.some.com за официальной информацией о зоне A.some.com, и, следовательно, все хосты, которые пользуются услугами этих серверов.

4) Атака на DNS-серверы зоны some.com. Используя динамическое обновление, злоумышленник изменяет базу данных зоны some.com на первичном сервере A.some.com. В этом случае весь Интернет будет пользоваться данными зоны A.some.com, сфальсифицированными злоумышленником.

Защита DNS. Для обеспечения подлинности адресн ой информации и достоверной передачи DNS-данных в системуDNS вводятся расширения, называемые DNSSEC (англ. *DomainNameSystemSecurityExtensions*) [4]. Основная идея DNSSEC состоит в использовании асимметричного шифрования для присоединения цифровой подписи к передаваемым данным, что обеспечивает проверку достоверности данных системы DNS и полученного от нее ответа. То есть, DNSSEC демонстрирует подлинность сайта и самой информации (контента), которая там находится, однако при этом не обеспечивается доступность данных и конфиденциальность запросов которая представлена на рисунке 1 [5].

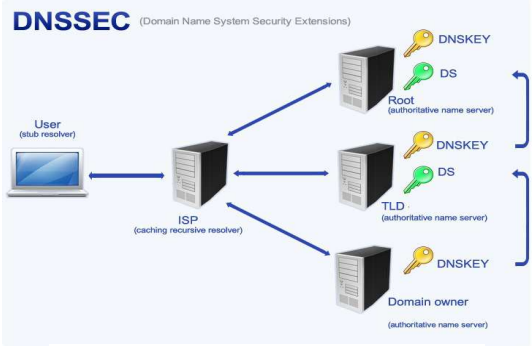

Рис. 1. Использование DNSSEC

В ходе исследования создана корпоративная сеть на основе продукта компании Microsoft Windows Server 2008 R2 с развернутым DNS сервером, в которой рассмотрен механизм обеспечения защиты DNSSEC, который представляет собой собрание расширений, повышающих надежность DNS протокола и обеспечивающих авторизацию происхождения данных и отрицание существования при проверке подлинности для DNS. Рассмотрены и реализованы два варианта операции подписания DNS-зон, отличающиеся друг от друга – подпись зоны, хранящейся в текстовом файле, и подпись зоны, хранящейся в Active Directory, что приведет к тому, что все записи для этой зоны тоже являются подписанными, после чего DNS-клиент может использовать цифровые подписи добавленные к записям ресурсов, для проверки их подлинности. Также рассмотрен принцип работы DNSSEC, в основе которого лежит использование двух типов ключей — одним подписывается зона (ZSK, zonesigningkey), другим подписывается набор ключей (KSK, keysigningkey).

Практическая значимость работы заключается в том, что предложенные методы позволяют, лучше защитить передаваемые DNS данные в сети и предотвратить их подделку, которая представляет собой очень опасную форму атаки, если ее инициировать с должным уровнем умений и злоумышленными намерениями. Предложенные методы позволяют защитить данные от атак осуществляемых методами фишинга для хищения учетных данных, установки вредоносного ПО и атак отказа нормальной работы (dos).

Литература

1. Мамаев М. Технологии защиты информации в Интернете / М. Мамаев, С. Петренко // СПб: Питер, 2002. – 198 с.

2. The successful deployment of DNSSEC requires the support of the entire Internet community. – Режим доступа: http://www.verisigninc.com/en_US/why-verisign/innovation-initiatives/dnssec/index.xhtml?loc=en_US . – Загл. с экрана.

3. Атака на ДНС. // [Персональная страница Карпова Г.] - Режим доступа: http://www.hackzone.ru/articles/dns-poison.html. – Загл. с экрана.

4. DNS – под прицелом", И. Медведовский, журнал "LAN/Журнал сетевых решений", 05/1997,URL: http://www.osp.ru/lan/1997/05/99.html. – Загл. с экрана.

5. Источники уязвимости DNS. – Режим доступа: //http://www.dnssec.ru/ru/exploits.php. – Загл. с экрана.