АТАКИ С ИСПОЛЬЗОВАНИЕМ DNS ПРОТОКОЛА И ПРОТИВОДЕЙСТВИЕ ИМ

Ф.Т. Борботько

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Для обращения к веб-ресурсам широко используется протокол прикладного уровня DNS, который применяется для преобразования доменных имен в IP-адреса серверов, на которых находятся эти ресурсы. Таким образом, отказ в работе DNS-сервера или сфальсифицированные данные, полученные от него могут привести к невозможности получить доступ к веб-ресурсу.

Для передачи DNS сообщений в основном используется протокол UDP, что существенно облегчает выполнение атак, при которых реализуется подмена ответов от сервера. Достаточно перехватить запрос и послать ответ от имени сервера. После приема такого пакета ответы от сервера будут отбрасываться, так как порт, на который пришел ответ от нарушителя, будет закрыт. На DNS-сервера можно проводить атаки методом «отравления кеша», путем заполнения его ложными записями. Атаки типа отказа в обслуживании (DoS) выполняются путем создания большого количество запросов на поиск адресов случайных доменных имен, в результате чего DNS-сервер будет вынужден обрабатывать только эти запросы.

Для защиты от прослушивания DNS трафика может быть использован DoT (DNS-over-TLS), суть которого заключается в установлении TLS соединения между отправителем и получателем. Также может быть реализован DoH (DNS-over-HTTPS), который передает зашифрованные запросы на преобразование имен через HTTPS соединения, в результате чего такие пакеты выглядят как любые другие веб-запросы. Для защиты от атак на DNS-сервера путем «отравления кеша» может быть использован DNSSEC, который обеспечивает проверку подлинности записей, полученных от серверов более высокого уровня. Это реализуется за счет использования двух ключей. Секретным ключом подписывается запись, а открытым ключом, который содержится в DNS-ответе проверяется подлинность и целостность этой записи.

Список литературы

1. Руководство по безопасности DNS / Habr.com [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/varonis/articles/519108/. – Дата доступа: 30.04.2023.

2. Анализ основных атак на DNS-сервер и методы использования DNSSEC при защите DNS-сервера / Cyberleninka.ru [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/analiz-osnovnyh-atak-na-dns-server-i-metody-ispolzovaniya-dnssec-pri-zaschite-dns-servera/viewer. – Дата доступа: 30.04.2023.