

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ АТАКАМ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА DNS

Н.Р. Коляго, Д.Н. Одинец

Атаки с использованием инфраструктуры DNS в основном относятся к DoS атакам. К ним можно отнести «отраженные» атаки и «отраженные» атаки с усилением. Эффективных способов защититься от таких атак нет. Фильтрация пакетов позволяет лишь частично ослабить воздействие.

Также с помощью DNS можно произвести разведывательную атаку. Обычно она является частью какой-то другой атаки. Защититься от нее можно только путем недопущения хранения чувствительной информации в системе DNS.

Протокол DNS разрабатывался с идеей общедоступности, никакой аутентификации пользователя или шифрования данных не предусмотрено. Кроме того, он реализован с помощью протокола UDP.

Обновление записей в реальном времени или по запросу является основной функцией DDNS (Dynamic DNS). Злоумышленник, подменив адрес в пакете DNS, мог добавить на сервер новую запись либо обновить существующую.

Отравление кэша (атака Каминского) [1] эксплуатирует отсутствие существенной проверки источника ответов и отсутствие установки соединения в протоколе UDP. Она позволяет подменить ресурсную запись в кэше рекурсивного сервера

DNS трафик может быть модифицирован Интернет-провайдером. Для защиты от таких атак были разработаны расширения DNSSEC и экспериментальный протокол DoH (DNS over HTTPS), которые обеспечивают надежность. Также DNS-серверы уязвимы перед DoS атаками случайного поддомена и NXDOMAIN атаками. Они заключаются в трате ресурсов на заведомо бесполезный поиск адреса. От таких атак, как и от других DoS невозможно полностью защититься, можно лишь смягчить воздействие путем оптимизации программного кода сервера и фильтрации входящих пакетов [2].

Литература

1. The Hitchhiker's Guide to DNS Cache Poisoning [Electronic resource]. – Access mode: https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. – Date of access: 15.03.2020.

2. DNS Amplification Attack Detection and Mitigation via sFlow with Security-Centric SDN /
A. Atan [et al.] // IMCOM '17. – 2017. – P. 1–7.